Surveon Control Center

Version1.0

User Manual

Release 1.1

About This Document

This document provides an overview of Server surveillance functionality, and details on how to operate and monitor a Server network using the Serveon Control Center. It is targeted at Server network administrators and security personnel tasked to monitor a surveillance area using the Server software.

Version History

Version	Description	Date
1.0	Initial release	November 2013
1.1	Remote Monitoring Modified	June 2014

All Rights Reserved © Surveon Technology 2014

Copyright Statement

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written consent of Surveon Technology Inc.

Disclaimer

Surveon Technology makes no representations or warranties with respect to the contents hereof and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Surveon Technology reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation to notify any person of such revisions or changes. Product specifications are also subject to change without notice.

Trademarks

Surveon and Surveon logo are trademarks of Surveon Technology Inc. Other names prefixed with “SMR” and “EMR” are trademarks of Surveon Technology Inc.

- Microsoft Windows and Windows are registered trademarks of Microsoft Corporation.
- Linux is a trademark of Linux Torvals.
- Solaris and Java are trademarks of Sun Microsystems, Inc.

All other names, brands, products or services are trademarks or registered trademarks of their respective owners.

Table of Contents

About This Document 2

Version History 2

All Rights Reserved © Surveon Technology 2014 3

Copyright Statement 3

Table of Contents 4

Chapter 1. Software Overview 18

1.1. Introduction 18

1.2. Module Framework 19

1.3. Hardware Requirements 21

1.4. System Architecture 22

1.4.1. Multiple Servers + SCC Client 23

1.4.2. Multiple Servers + SCC Client + Matrix Wall Client 24

1.4.3. Network Requirements 25

Configuring Windows Firewall Exceptions 25

Opening Ports 26

Warnings / Precautions 26

1.4.4. Windows Vista/7 User Notes 27

1.5. Port Forwarding 28

1.5.1. Port Forwarding for Accessing SCC Server 29

1.6. Installing the SCC 32

1.7. Starting the SCC Client 39

1.7.1. Checking the Software Version 40

1.7.2. Logging out 40

Chapter 2. Basic System Settings 41

2.1. Adding NVRs to the Server 41

2.1.1. Automatic Scan for NVRs 41

2.1.2. Manually adding NVRs 43

2.2. Storage Management 45

2.3. Adding Cameras to the Server 47

2.3.1. Automatic Scan for Cameras 47
2.3.2. Manually Adding Cameras 50
2.4. Setting Recording Schedule 52
2.4.1. Weekly Scheduling 52
2.4.2. Daily Scheduling 54
2.5. Adding Alarm Rules 55
2.6. Setting up Live View 57
Chapter 3. Live View 58
3.1. Live View Window Overview 58
3.1.1. Resizing and Minimizing Windows 60
Minimizing Controls 60
Hiding and Showing the Explorer Area 60
3.2. View Setup 61
3.2.1. Types of Views 61
3.2.2. Add View 62
3.2.3. Add PAP View 63
3.2.4. Add Fisheye View 64
3.2.5. Renaming a View 65
3.2.6. Deleting a View 65
3.2.7. Sending View to a New Window 65
3.2.8. Switching Between Views 66
3.2.9. Switching Between Different Screen Divisions 66
Creating and Using New Screen Divisions 66
Screen Division Page Use 66
Auto-flipping Pages 67
Configuring Page Dwell Time 67
Exiting Different Screen Divisions 67
3.3. Functionality Within Views 68
3.3.1. Digital Zoom 68
3.3.2. Instant Playback 69
3.3.3. Manual Recording 72

3.3.4. Preset Pan 72
3.3.5. Stream Selection 72
3.3.6. Image Settings 72
3.3.7. Video Ratio Adjustment 73
3.3.8. Inserting Overlays 73
Image Overlay 73
HTML Overlay 74
3.3.9. Send to Large Channel 74
3.3.10. Reconnect 75
3.3.11. Remove the Camera 75
3.3.12. Onscreen PTZ Control 76
Pan and Tilt 76
Zoom 76
3.4. Full Screen View 77
3.4.1. Entering Full Screen View 77
3.4.2. Exiting Full Screen Mode 77
3.5. E-Maps 78
3.5.1. Adding E-Maps 78
3.5.2. Adding Sub-Maps 78
3.5.3. Adding Additional E-Maps 79
3.5.4. Changing E-Map Order 80
3.5.5. Renaming an E-Map 80
3.5.6. Configuring an E-Map 80
3.5.7. Deleting an E-Map 81
3.5.8. Using the E-Map 81
Chapter 4. Server Setup 83
4.1. Server Basic Functions 83
4.1.1. Logging into a Server 83
4.1.2. Logging out of a Server 83
4.1.3. Renaming a Server 84
4.1.4. Viewing Server and Client Information 84

4.2. Server Settings 85
4.2.1. General Server Settings 86
4.2.2. To perform Notification Setting 88
4.2.3. Pre/Post Alarm Recording Settings 90
4.2.4. Storage Management 91
4.3. Scheduling Recording 94
4.3.1. Global Scheduling 94
Weekly Global Scheduling 94
Daily Global Scheduling 96
4.3.2. Individual Scheduling 97
Weekly Individual Scheduling 97
Daily Individual Scheduling 99
Chapter 5. Camera Setup 101
5.1. Adding Cameras 101
5.1.1. Automatic Scan for Cameras 101
5.1.2. Manually Adding Cameras 104
5.1.3. Deleting a Camera 105
5.1.4. Initializing a Camera 106
5.2. Camera General Settings 107
5.2.1. Logging into a Camera 107
5.2.2. Changing the Camera Model and Vendor 107
5.2.3. General Settings 109
5.2.4. OSD Settings 110
5.2.5. Privacy Mask Settings 111
5.3. Camera Image and Quality Settings 113
5.3.1. Camera Image Settings 113
5.3.2. Advanced Video Settings 114
5.4. PTZ Settings 115
5.4.1. PTZ Settings 115
5.4.2. PTZ Preset Settings 116
Adding a Preset 116

Deleting a Preset 117
5.4.3. PTZ Patrol Settings 117
5.5. PTZ Controls 119
5.5.1. Directional Pad 119
Pan and Tilt 119
Zoom 119
5.5.2. Functional Buttons 120
Speed 120
Home 120
Preset 120
Adding a Preset 120
Deleting a Preset 120
Start Auto Pan 121
Focus 121
Chapter 6. Alarms and Events 122
6.1. Camera VI Detection Settings 123
6.1.1. General Motion Detection 124
Configuring and Editing Detection Windows 124
Testing Detection Windows 125
Deleting a Detection Window 125
Enabling or Disabling a Detection 125
Opening the Help File 125
6.1.2. Foreign Object Detection 126
Configuring and Editing Detection Windows 126
Testing Detection Windows 127
Deleting a Detection Window 127
Enabling or Disabling a Detection 127
6.1.3. Forbidden Area Detection 129
Configuring and Editing Detection Windows 129
Testing Detection Windows 130
Deleting a Detection Window 130

Enabling or Disabling a Detection 130
Opening the Help File 131
6.1.4. Intrusion Detection 132
Configuring and Editing Detection Windows 132
Testing Detection Windows 133
Deleting a Detection Window 133
Enabling or Disabling a Detection 133
Opening the Help File 134
6.1.5. Missing Object Detection 135
Configuring and Editing Detection Windows 135
Testing Detection Windows 136
Deleting a Detection Window 136
Enabling or Disabling a Detection 136
Opening the Help File 137
6.1.6. Tampering Detection 138
Configuring Tampering Detection 138
Testing Tampering Detection 139
Enabling or Disabling a Detection 139
Opening the Help File 139
6.1.7. Camera Motion Detection 140
Configuring and Editing Detection Windows 140
Deleting a Detection Window 141
Opening the Help File 141
6.1.8. Virtual Fence 142
Configuring and Editing Detection Windows 142
Testing Detection Windows 143
Deleting a Detection Window 143
Enabling or Disabling a Detection 144
Opening the Help File 144
6.1.9. Object Counting 145
Configuring and Editing Detection Windows 145

Testing Detection Windows 146
Deleting a Detection Window 147
Enabling or Disabling a Detection 147
Opening the Help File 147
6.1.10. Going Out Detection 148
Configuring and Editing Detection Windows 148
Testing Detection Windows 149
Deleting a Detection Window 149
Enabling or Disabling a Detection 149
Opening the Help File 150
6.1.11. Tailgating Detection 151
Configuring and Editing Detection Windows 151
Testing Detection Windows 152
Deleting a Dividing LIne 152
Enabling or Disabling a Detection 152
Opening the Help File 153
6.2. Alarm Rules 154
6.2.1. Adding an Alarm Rule 155
Alarm Conditions 155
Alarm Actions 158
Alarm Scheduling 164
6.3. Alarms View and Notification 166
6.3.1. Live View Event Log 166
6.3.2. Alarm Popups 167
Setting Popup Sleep Time 168
6.3.3. Video Panel 169
Playback from Video Alarm Panel 169
Tagging an Alarm Thumbnail 170
6.4. Event Log 171
6.4.1. Exporting a Log 172
6.4.2. Searching the Event Log 172

System Type 172
Event Type 173
Operation Type 174
Performing a Search 174
6.4.3. Event Log Setup 175
6.4.4. Log for Object Counting 175
6.4.5. Event Log View 177
Chapter 7. Search and Playback 178
7.1. Introduction 178
7.2. Date/Time Search 179
7.2.1. Time Selection 179
Recent Time 179
Specified Time 179
7.2.2. Use of 1x/4x Views 180
7.2.3. Camera Selection 180
7.2.4. Timeline 181
7.2.5. Playback 183
Synchronized Playback 185
Capturing Snapshot 185
Capturing Video Clip 186
7.3. VI Search 188
7.3.1. Creating a VI Search 189
Time Selection 189
Camera Selection 190
Setting New Search Criteria 190
General Motion Detection 191
Tampering Detection 192
Intrusion Detection 193
Missing Object Detection 195
Foreign Object Detection 197
Forbidden Area Detection 200

Virtual Fence 202
Going Out Detection 203
Tailgating Detection 205
7.3.2. Saving/Retrieving a VI Search 206
7.3.3. Using the Search Results 206
Selecting the Result 206
Result Playback 207
Playback Synchronization 208
Capturing Snapshot 208
Capturing Video Clip 209
Logging and Noting 210
Label Setup 210
7.4. Event Search 211
7.4.1. Creating an Event Search 212
Time Selection 212
Camera Selection 213
Setting Event Search Criteria 213
7.4.2. Using the Search Results 214
Selecting the Result 214
Result Playback 215
Playback Synchronization 216
Capturing Snapshot 216
Logging and Noting 217
Chapter 8. Remote Web Client and SPhone Client for Simple Use (Optional) 218
8.1. Starting the Web Client 219
8.1.1. Checking the Software Version 219
8.1.2. Use of 1x/4x views 219
8.1.3. PTZ Control 220
8.1.4. Playback Settings 220
8.2. Installing and Starting the SPhone Client on iOS Devices 221
8.2.1. Installing the SPhone Client (Optional) 221

8.2.2. Starting the SPhone Client 221
8.2.3. Checking the Software Version 222
8.2.4. Live View/Playback on the SPhone Client 222
8.3. Installing and Starting the SPhone Client on Android Devices 225
8.3.1. Installing the SPhone Client (Optional) 225
8.3.2. Starting the SPhone Client 225
8.3.3. Checking the Software Version 226
8.3.4. Live View on the SPhone Client 226
Chapter 9. Matrix Wall Client 228
9.1. Matrix Slave 228
9.1.1. Add Video Station 228
9.2. View Explorer on Matrix Page 230
9.2.1. View 230
Add View 230
Renaming a View 231
Deleting a View 231
9.2.2. Mutli-Monitor in One (TV Wall) 232
Screen Division Page Use 235
Chapter 10. System Setup 236
10.1. Settings Under SMR / NVR Server 236
Common Server Tasks 237
Alarm Rule Settings 237
View Log 237
Global Schedule 237
Storage 237
E-map 237
Common Camera Tasks 237
Scan for Cameras 237
Add Cameras 238
Common Other Tasks 238
Account Manager 238

Camera Overview List 238
Disk Storage Overview 238
Recent Key Events 238
System Health History 239
System Status 239
10.2. Settings Under Server 240
10.2.1. General Tasks 241
Alarm Rule Settings 241
View Log 241
E-Map 241
Global Schedule 241
Individual Schedule 241
Storage 242
Pre/Post Alarm Recording Settings 242
Email 242
SMS 242
I/O Central Panel 242
Genera Server Settings 243
Joystick 243
10.2.2. Other Tasks 245
Reboot NVR Server 245
Schedule Reboot 246
Audio Input 246
Playback Camera List Setting 247
Playback Buffer 247
Auto Login 248
VI Panel 248
Lock Windows 248
Advance View Explorer 249
Import/Export 249
Importing Parameters 249

Exporting Parameters 249
Customize Logo 250
Router Port Mapping 250
10.3. Settings Under Camera List 251
10.3.1. General Tasks 251
Scan for Cameras 251
Add Cameras 251
Delete Camera 251
10.3.2. Camera Settings 252
Image Settings 252
Advanced Video Settings 252
General Camera Settings 252
Edit Camera 252
PTZ Settings 252
Preset Settings 253
OSD Settings 253
Mask Settings 253
Compatibility Verify 253
Initialize 253
Automatic Settings 253
10.3.3. Video Analytics 254
General Motion Detection 254
Foreign Object Detection 254
Forbidden Area Detection 254
Intrusion Detection 254
Missing Object Detection 255
Tampering Detection 255
Camera Motion Detection 255
Virtual Fence 255
Object Counting 255
Going Out Detection 255

Tailgating Detection 255
10.4. Settings Under Ethernet I/O Box 256
10.4.1. General Tasks 256
Add Device 256
Edit Device 258
Delete Device 258
10.5. Settings Under Account Manager 259
10.5.1. Account List 259
Adding an Account 260
Editing an Account 261
Changing an Account Password 262
Deleting an Account 262
10.5.2. Functional Authority 263
10.6. Settings Under Network Parameters 264
10.6.1. Main Tasks 264
Maximum Video Connections 264
Blacklist/Whitelist Settings 265
Edit NVR 266
Web Server 266
Multiple LAN Support 267
DHCP Server 267
10.7. Settings Under Others 269
10.7.1. Other Tasks 269
Import/Export 269
Resolution 270
Language 271
Help 271
About 271
10.8. Settings Under Domain Server 272
Tasks 272
Auto Scan NVR 272

Add NVR 273
Edit NVR 273
Delete NVR 273
IO Button On Screen Setting 274
Account Manager 275
DDNS Setting 276
Import/Export 276
Help 276
About 276
SCC Software License Mechanism 277

Chapter 1. Software Overview

1.1. Introduction

The Surveon Control Center (SCC) is a complete solution for large-scale and high level enterprise projects. It can manage product including SMR Series, NVR Series, VMS server and Matrix server, and support unlimited numbers of cameras, I/O devices, SMR/NVR/VMS/Matrix servers and users. SCC allows multiple clients to manage multiple servers performing monitoring, recording, and playback over different servers. For users having multiple SMR/NVR/VMS/Matrix Servers, SCC can be utilized to manage over the domain infrastructure.

1.2. Module Framework

- VMS/NVR Server
  - Combines video recording, archival and retrieval functionalities for individual servers/standalone PCs.
  - Serves as the connection point for client stations.
- Local Domain Server
  - The interface between the VMS/VI Servers and any clients.
  - User authentication server.
- Local Client
  - Local access, VMS Client installed on standalone PCs/SMRs for live video monitoring, event recording playback access and VMS system configuration.
- Remote Client (full functions)
  - Remote access, VMS Client installed on remote PCs for live video monitoring, event recording playback access.
  - Serves as the default configuration point for NVR2000 series, which do not have a Local Client.
- Web Client (for simple use)
  - Remote access, an ActiveX application (OCX) installed on remote PCs for live viewing and event playbacks through the web browser.
- SPhone Client (for simple use)
  - SPhone Client installed on iOS/ Android devices for basic live viewing.
- Web Server
  - Allows user to access the live video stream, PTZ control and event recording playbacks through Microsoft Internet Explorer 7.0 (or higher) after the Web Clients components are downloaded.
- VI Server
  - The video intelligence processing point for a VMS solution.
  - Preinstalled on SMR/NVR Server, and optional on a separate server/PC (VMS).
- SCC Domain Server
  - Allows centralized control over multiple Trusted VMS Server points and connections from multiple clients.

- SCC Client
  - Software capable of accessing multiple Trusted VMS Servers through the SCC Domain Server.
- Matrix Wall Client
  - Allows users to manage and display videos in numerous monitors and multiple-monitors in one (matrix TV wall).

1.3. Hardware Requirements

These are the hardware requirements for using PCs as Server or Client.

SCC Server	**≤20**	**Unlimited**
Operating System	64-bit : Windows 7 Ultimate / - Enterprise / - Professional	
CPU	Intel Core i3 3.3GHz or above	Intel Core i7 3.4GHz or above
RAM	4 GB or above	
Display Card	nVidia GeForce GT610 1GB or above	
Hard Drive	SATA 7200 RPM, 500 GB or above	
Network Interface	1Gbps or above	
SCC Client **(+Matrix Wall Client)**	**≤20**	**Unlimited**
Operating System	64-bit : Windows 7 Ultimate / - Enterprise / - Professional	
Operating System	Intel Core i7 3.4GHz or above	
RAM	4 GB or above	
Display Card	nVidia GeForce GTX 660 2GB or above	
Hard Drive	SATA 7200 RPM, 500 GB or above	
Network Interface	1Gbps or above	

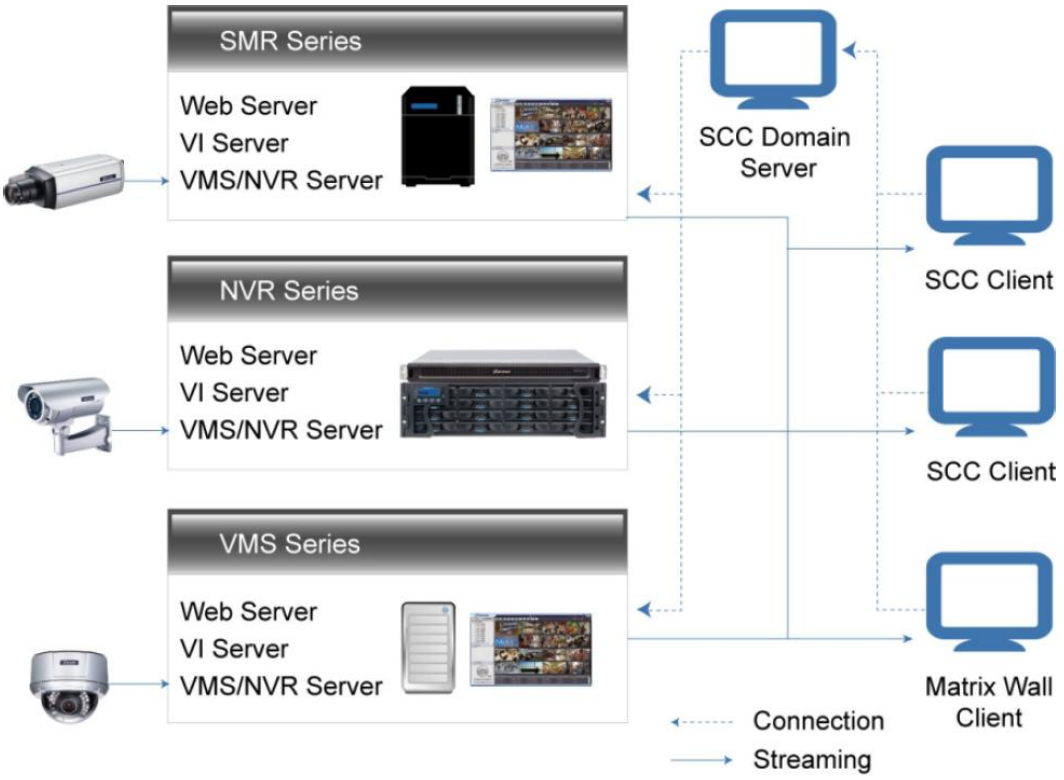
1.4. System Architecture

SCC operates in scalable client - server architecture. This architecture can be divided into two types: (1) Multiple Servers + SCC Client and (2) Multiple Servers + SCC Client +Matrix Wall Client.

The comparisons between SCC Client and SCC Client + Matrix Wall Client:

Items	SCC Client	SCC Client + Matrix Wall Client
Utilization	Multiple servers & multiple client surveillances at the same time.	
	<100 cameras project	200+ cameras project
		TV-Wall (Multi-Monitors)
Support Multi-NVR	Yes	Yes
Central/Remote Mgt.	Yes	Yes
Central Alarm & Event Mgt.	Yes	Yes
TV-Wall Mgt.	N/A	Yes
Virtual Matrix	Yes (Max. 8)	Yes (unlimited)
Maximum Monitor	8 on single client	Unlimited
Maximum Video View	72CH on single client	Unlimited
SCC Client	Unlimited	Unlimited
SCC License	By # of NVR	By # of NVR

1.4.1. Multiple Servers + SCC Client



[SCC Domain Server]

Install the SCC Domain Server on a PC.

1. Insert the SCC product CD
2. Click SCC Suite on the menu to start the installation.
3. Choose Advanced Setup to select the SCC Domain Server only.

[SCC Client]

Install the SCC Client on PCs.

1. Insert the SCC product CD.
2. Click SCC Suite on the menu to start the installation.
3. Choose Advanced Setup to select the SCC Client only.

1.4.2. Multiple Servers + SCC Client + Matrix Wall Client

[SCC Domain Server]

Install the SCC Domain Server on a PC.

1. Insert the SCC product CD.
2. Click SCC Suite on the menu to start the installation.
3. Choose Advanced Setup to select the SCC Domain Server only.

[SCC Client]

Install the SCC Client on PCs.

1. Insert the SCC product CD.
2. Click SCC Suite on the menu to start the installation.
3. Choose Advanced Setup to select the SCC Client only.

[Matrix Wall Client]

Install the Matrix Wall Client on PCs.

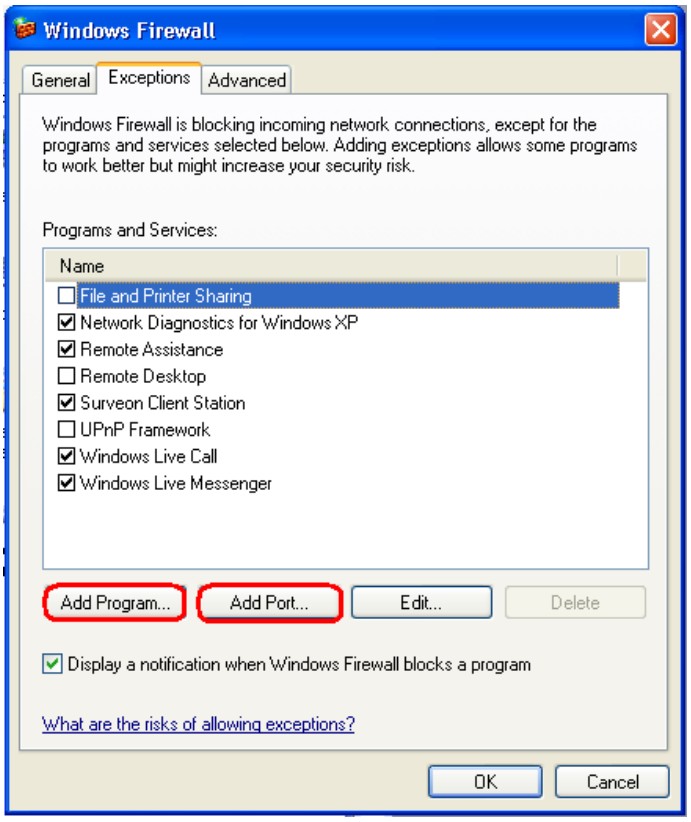
1. Insert the SCC product CD.
2. Click SCC Suite on the menu to start the installation.
3. Choose Advanced Setup to select the Matrix Wall Client only.

1.4.3. Network Requirements

In order to preserve enough bandwidth for surveillance video, a surveillance network is presumed to be free of user/business traffic. Server software currently supports Class B and Class C type addresses. Currently the Server software only searches for Servers on the same subnet. Cameras should also reside on the same subnet.

Configuring Windows Firewall Exceptions

The Windows firewall will block incoming network connections, so the SCC should be added to the firewall exceptions list. The instructions below are for Windows XP, however the process is similar under Vista and Windows 7.



1. Open **Settings > Control Panel > Windows Firewall.**
2. Under the *Exceptions* tab, click **Add Program…**
3. Click browse and go to your install directory.
4. Select NVRService.exe.
5. If you require DHCP services, repeat steps 3 and 4 and add dhcpsrv.exe
6. Click **OK** to save your settings.

Opening Ports

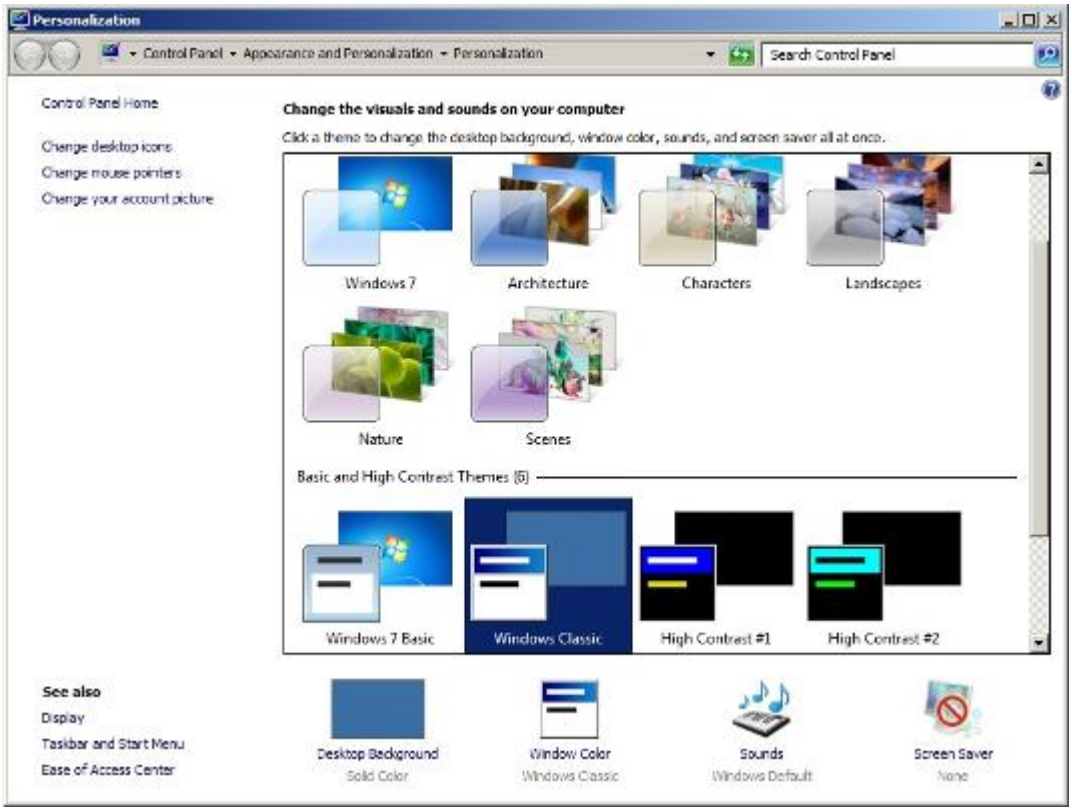
If access through a firewall in a local network is required, try opening the following ports: SMTP (25), HTTP (80), FTP (20, 21), OMNI (2809), HTTPS (443) and RTSP (554, 8554.). Other ports should also be opened while using port forwarding to access the SCC Server: Stream Port (9090), Doman Data Port (9060), Log Download Message Port (15507) and Log Download Data Port (9080).

Note: Please refer to *Port Forwarding* Section for more details.

Warnings / Precautions

If the Server and a SCC client reside on separate subnets, please set up gateway, VLAN, or cross-subnet routing to bridge surveillance traffic. Please consult with a network administrator for problems with network setups. A SCC client needs to be rebooted when network settings are changed.

1.4.4. Windows Vista/7 User Notes



Windows Vista and 7 users may experience problems with the video display/overlay when using certain themes. If you experience these problems, we recommend you change your theme to *Windows Classic* under **Control Panel > Appearance and Personalization > Personalization.**

In Windows Vista and Windows 7, User Account Control (UAC) is a security infrastructure that restricts application privileges. This feature must be disabled for the recording functionality of the SCC to work correctly. To disable UAC, first open a command prompt by selecting **All Programs> Accessories > Command Prompt.** At the command line, enter the following command:

C:\Windows\System32\cmd.exe /k %windir%\System32\reg.exe

ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f

To re-enable UAC use the following command:

C:\Windows\System32\cmd.exe /k %windir%\System32\reg.exe

ADD KLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 1 /f

1.5. Port Forwarding

Port forwarding is a name given to the combined technique of:

1. Translating the address and/or port number of a packet to a new destination.
2. Possibly accepting such packet(s) in a packet filter (firewall).
3. Forwarding the packet according to the routing table.

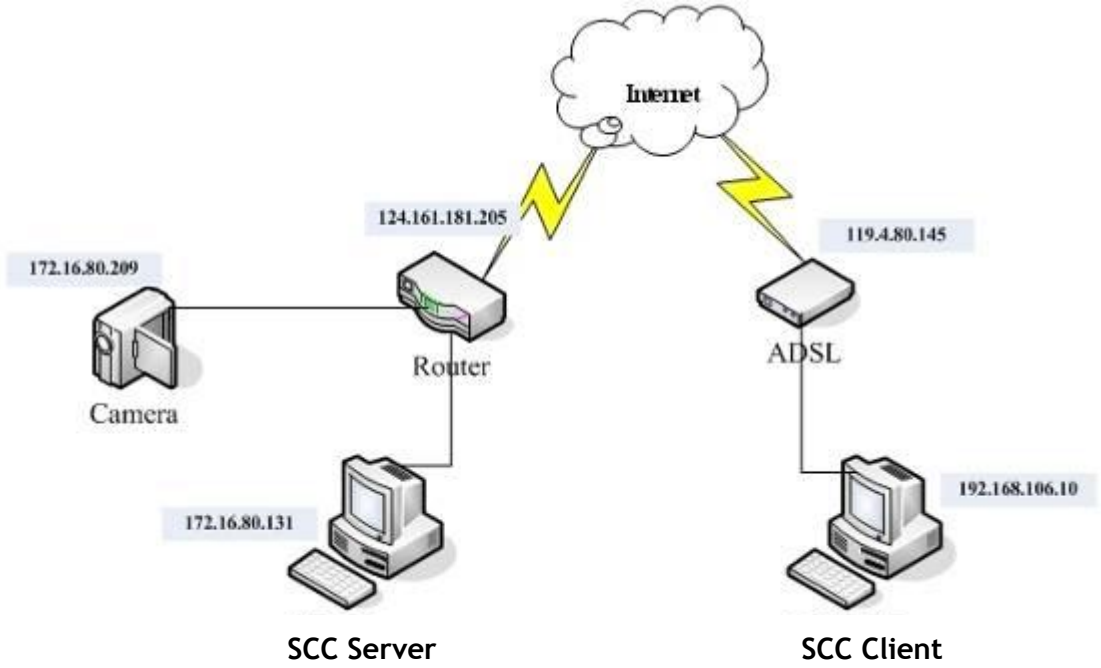
To illustrate its concept, two computers on the Internet that communicate with each other using TCP/IP or UDP/IP protocols(though the process is not limited to these) utilize ports to identify the opposite connection points of each other where the data packets supposed to go to. In order to communicate, each computer knows the port of another computer (in addition to IP address) and sends the data to that port. Port forwarding forwards these ports in such a way that when one computer sends data to the specific port of another computer, the data is actually sent to a different port. This allows remote computers to connect to a specific computer or service within a private LAN.

In a typical residential network, nodes obtain Internet access through a DSL or cable modem connected to a router or network address translator (NAT/NAPT). Hosts on the private network are connected to an Ethernet switch or communicate via a wireless LAN. The NAT device's external interface is configured with a public IP address. The computers behind the router, on the other hand, are invisible to hosts on the Internet as they each communicate only with a private IP address.

When configuring port forwarding, the network administrator sets aside one port number on the gateway for the exclusive use of communicating with a service in the private network, located on a specific host. External hosts must know this port number and the address of the gateway to communicate with the network-internal service.

When used on gateway devices, a port forward may be implemented with a single rule to translate the destination address and port. The source address and port are, in this case, left unchanged. When used on machines that are not the default gateway of the network, the source address must be changed to be the address of the translating machine, or packets will bypass the translator and the connection will fail.

1.5.1. Port Forwarding for Accessing SCC Server



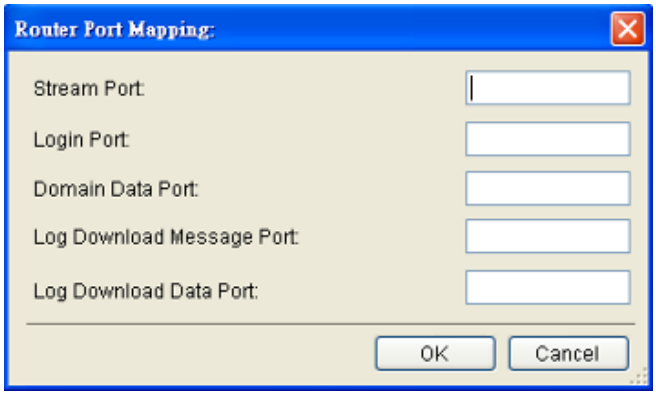
To enable port forwarding for accessing SCC Server, please follow the steps below:

1. Do Router Port Mapping for SCC/NVR Server

Go to ***Setup*** > ***Other Tasks*** > ***Server*** > ***Router Port Mapping*** in SCC after it is installed.

Note: The VMS/NVR Server is preinstalled in NVR2000/SMR Series.

A *Router Port Mapping* window will prompt for entering port numbers. Please put in the numbers as listed below:



Stream Port: 9090

Login: Port: 2809

Doman Data Port: 9060

Log Download Message Port: 15507

Log Download Data Port: 9080

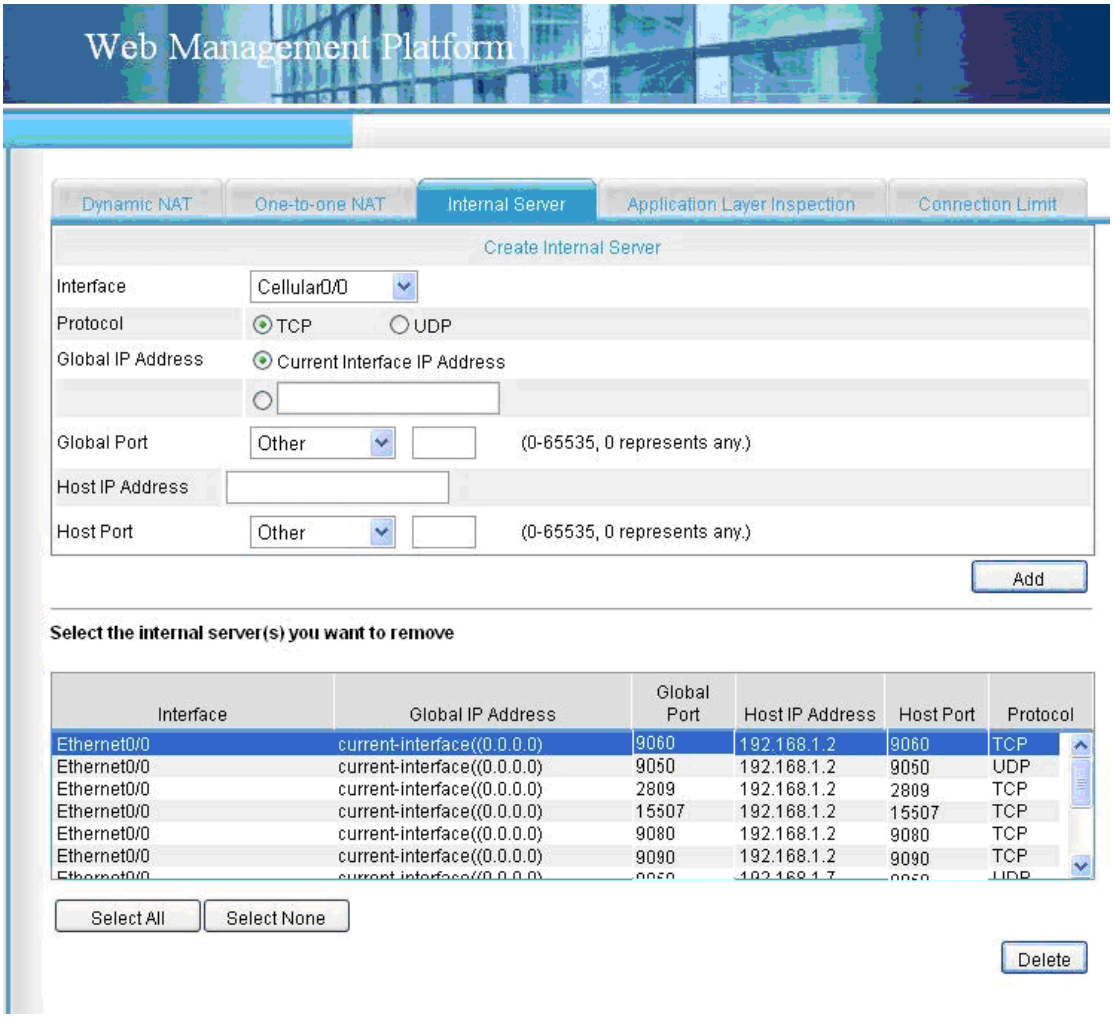
2. Open Ports on the Router

Host Ports: The private ports that the internal SCC/NVR Server use, which are unchangeable.

Global Ports: The public ports for remote clients to connect to the internal SCC/NVR Server. The Global ports are changeable, but the simplest way is to make them the same with the host ports.

Please open the listed ports on your router:

Port(Host/Global Port)	**Protocol**	**Port Number**
Domain Message Port	UDP	9050
Domain Data Port	TCP	9060
Login Port	TCP	2809
Stream Port	TCP	9090
Log Download Message Port	TCP	15507
Log Download Data Port	TCP	9080

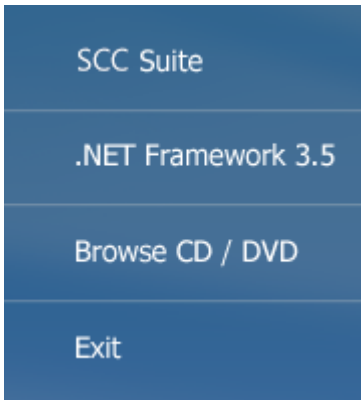


Note: Camera port (default: 80) and stream port (default: 6002) for accessing cameras should be opened while SCC/NVR Server and the cameras and are not in the same LAN.

1.6. Installing the SCC

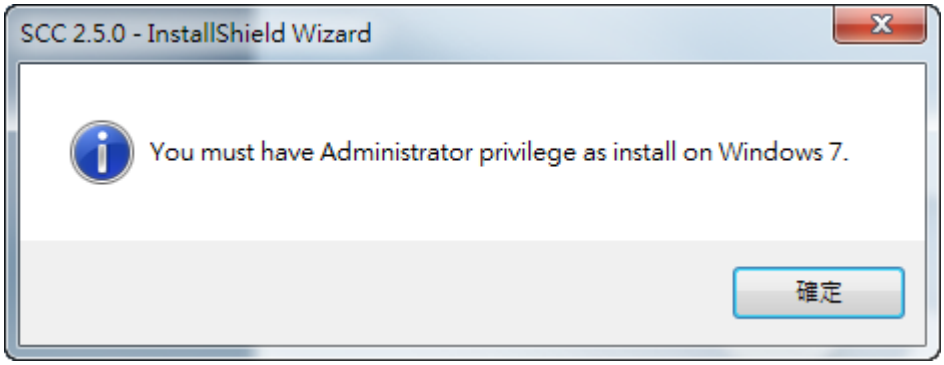
Note: For NVR2000/SMR series, users have to install SCC Client on remote PC(s) when distant live viewing and playback are needed.

1. Insert the SCC CD-ROM. The CD should autorun. If it does not, open the CD manually and double-click **autorun.exe**. The menu below will be displayed.

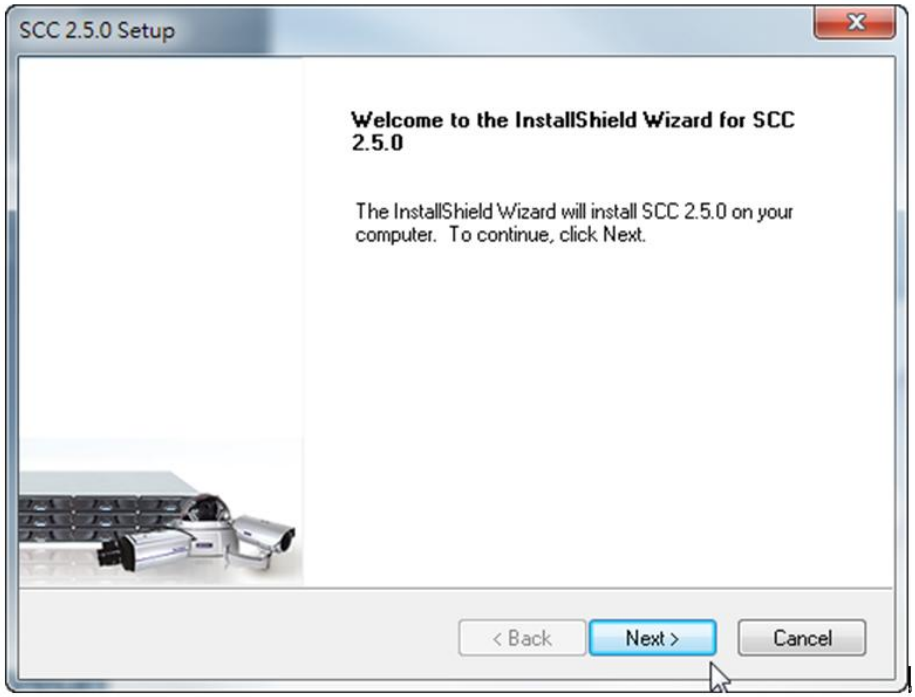


Click **SCC Suite** to start the installation.

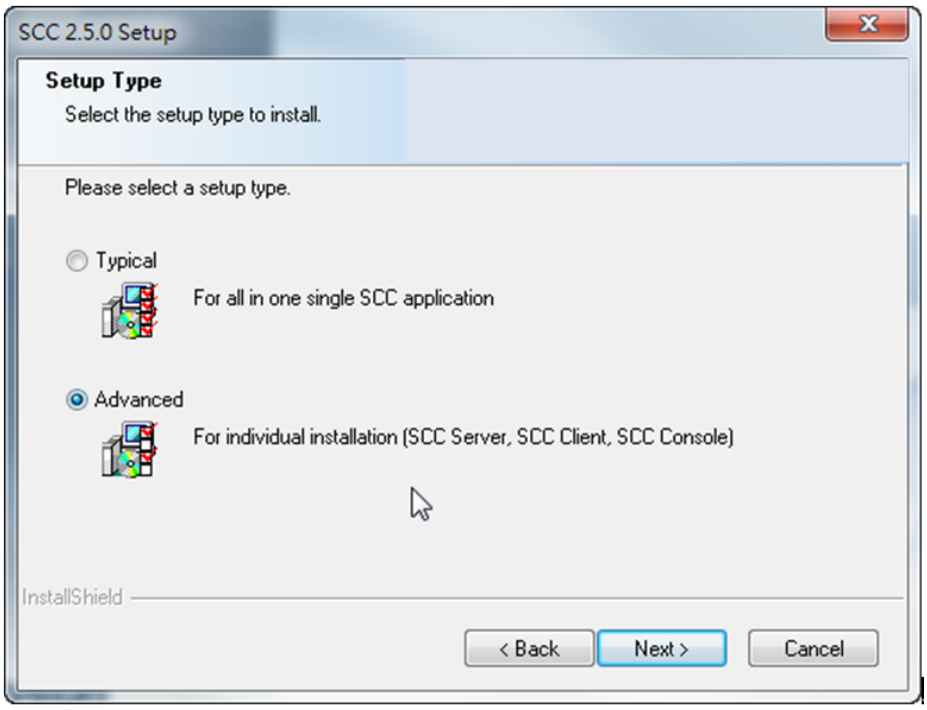
2. SCC will check your Administrator privilege for installation.



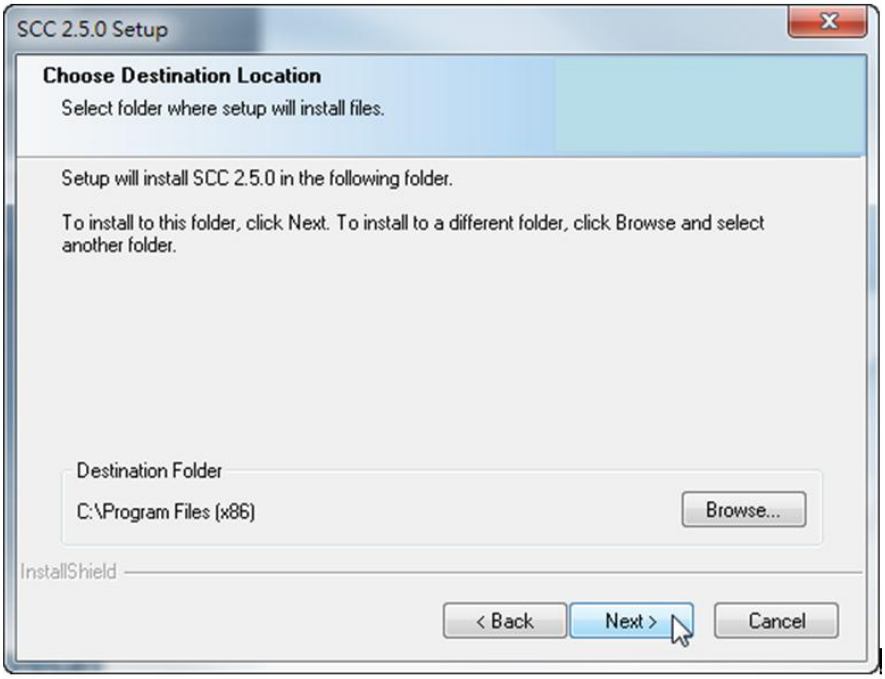
3. Once clicked Yes, the SCC InstallShield Wizard will appear.


SCC 2.5.0 Setup
Welcome to the InstallShield Wizard for SCC 2.5.0
The InstallShield Wizard will install SCC 2.5.0 on your computer. To continue, click Next.
< Back
Next >
Cancel

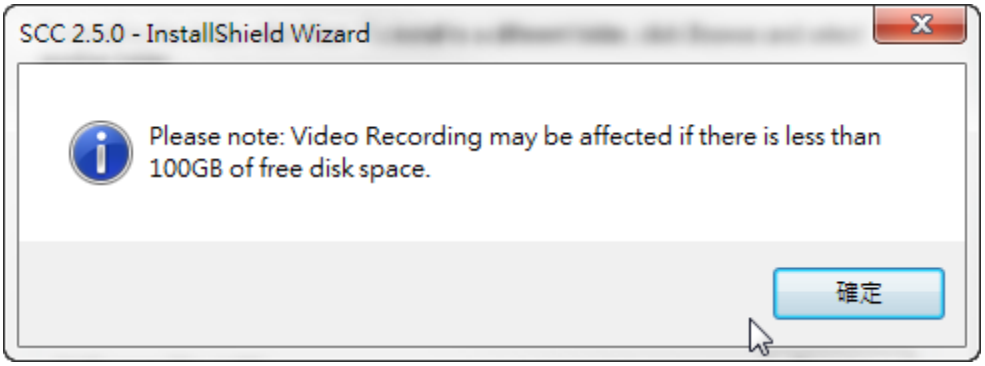
4. Choose a setup type from *Typical* and *Advanced*. Then Click **Next** when you are satisfied with your selection.



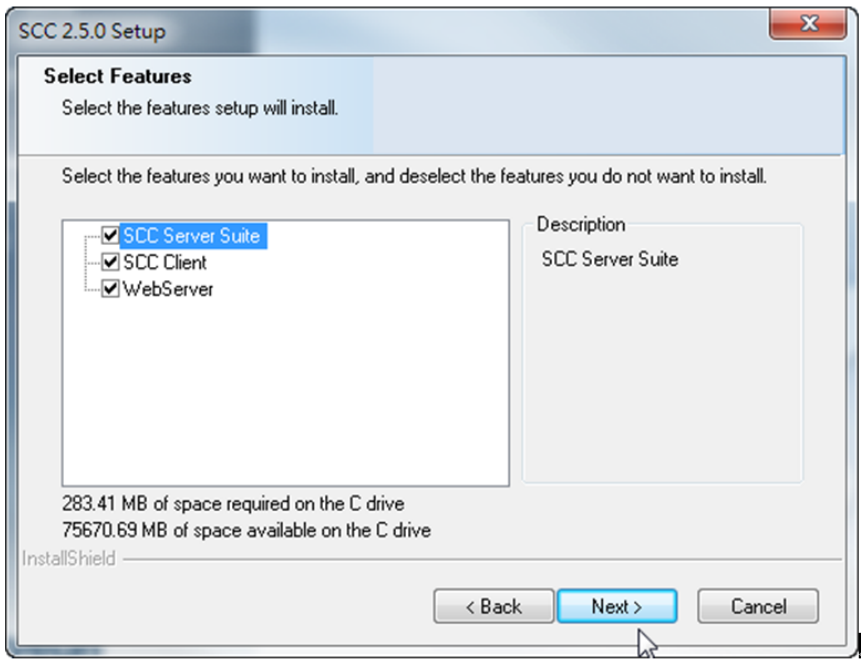
5. You can choose the folder for SCC installation files.


SCC 2.5.0 Setup
Choose Destination Location
Select folder where setup will install files.
Setup will install SCC 2.5.0 in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\Program Files (x86)
Browse...
InstallShield
< Back
Next >
Cancel

6. A notice will come out.

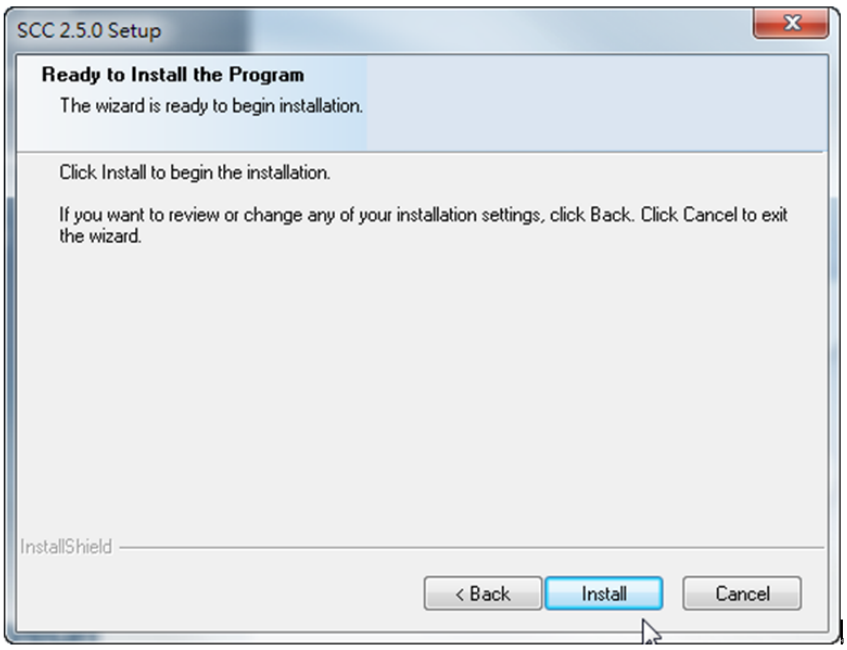

SCC 2.5.0 - InstallShield Wizard
Please note: Video Recording may be affected if there is less than 100GB of free disk space.
確定

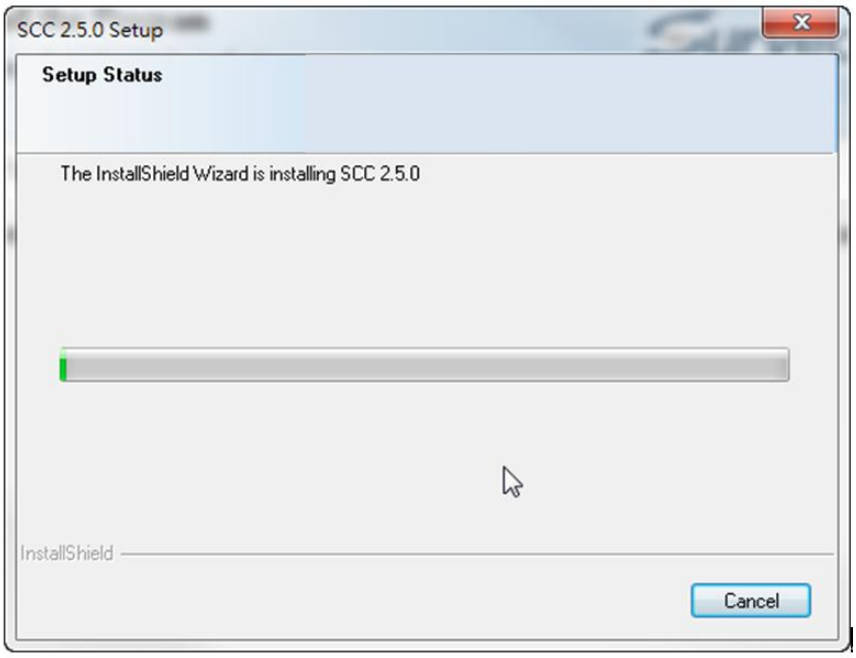
7. You may choose to install among the following while *Advanced Setup Type* is selected:


SCC 2.5.0 Setup
Select Features
Select the features setup will install.
Select the features you want to install, and deselect the features you do not want to install.
SCC Server Suite
SCC Client
WebServer
Description
SCC Server Suite
283.41 MB of space required on the C drive
75670.69 MB of space available on the C drive
InstallShield
< Back
Next >
Cancel

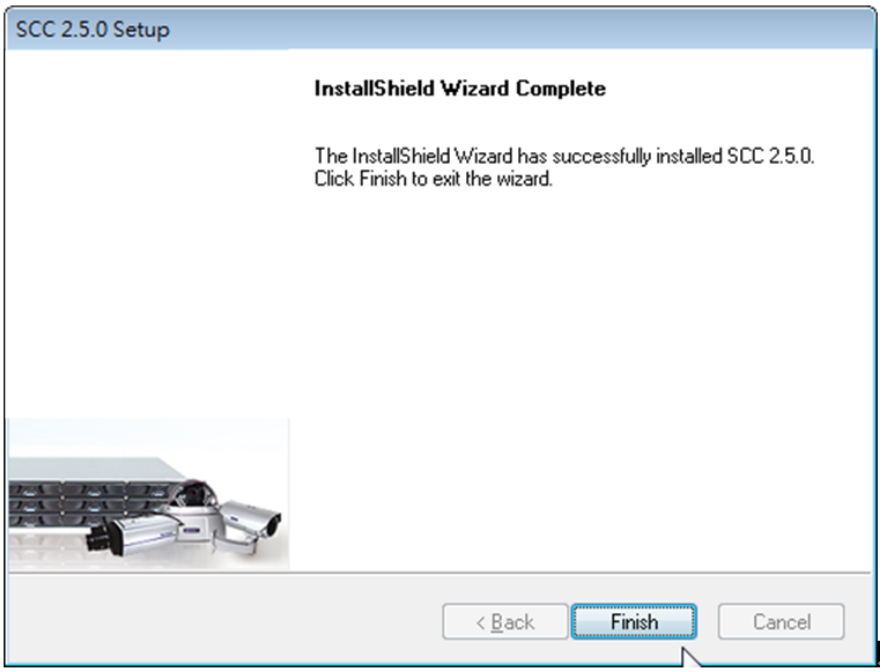
- **SCC Server Suite** – Includes the SCC Server and Local Domain Server, VI Server and VMS Client.
- **SCC Client**
- **Web Server**

8. The confirmation screen will display. Click **Install**. A progress bar will display, indicating installation progress.

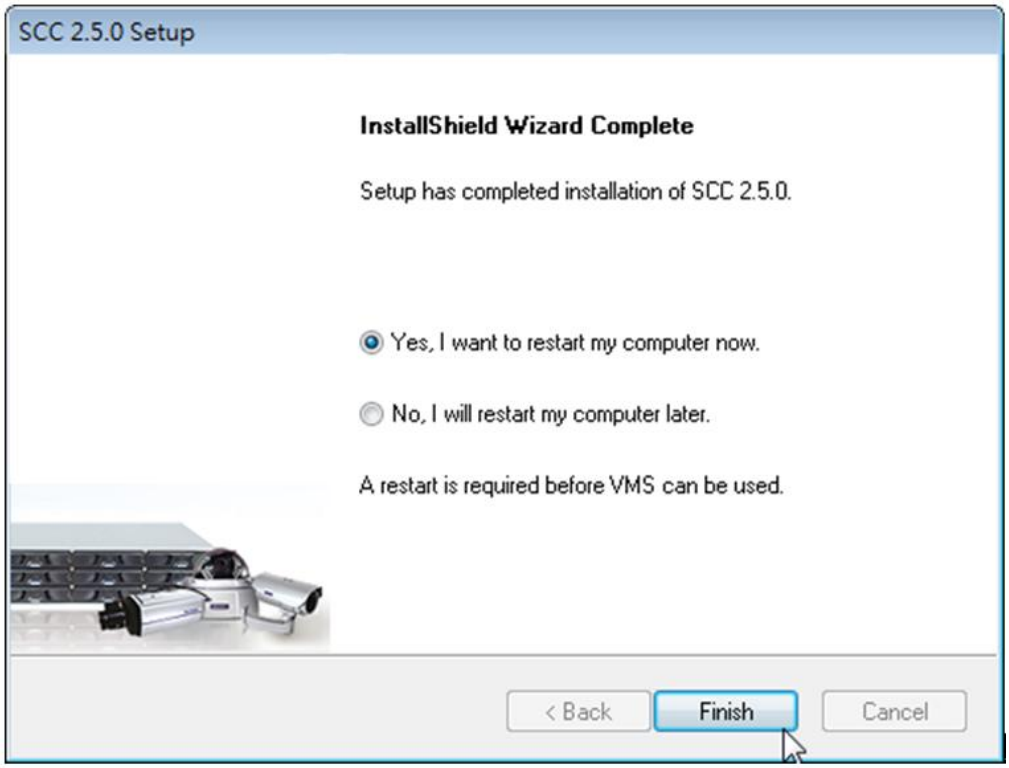

SCC 2.5.0 Setup
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel



9. When installation is finished, an informational screen will display. Click **Finish** to complete installation.



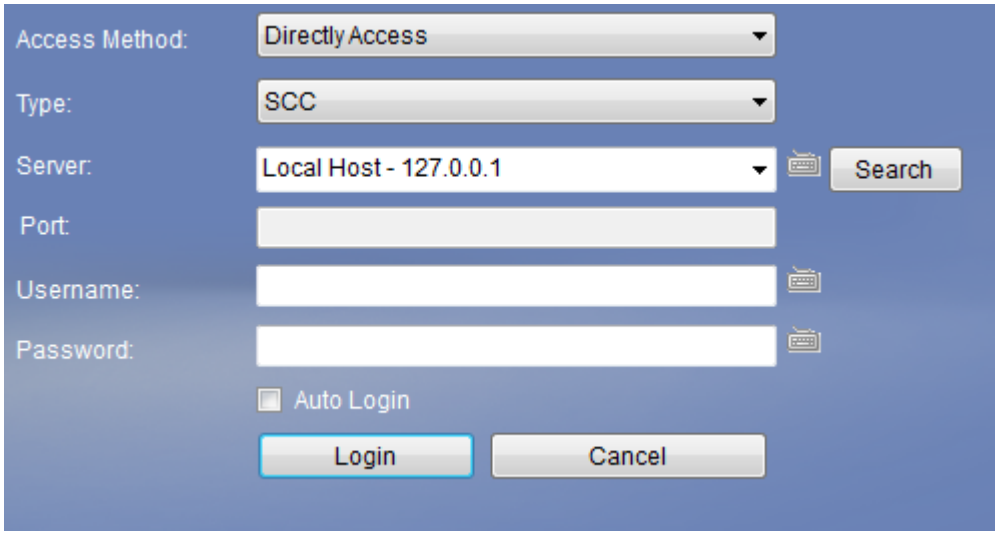
The system will prompt for a restart. A restart is required before the SCC will function correctly. You may choose to immediately automatically restart your computer, or restart your computer later. Clicking **Finish** will apply your choice.


SCC 2.5.0 Setup
InstallShield Wizard Complete
Setup has completed installation of SCC 2.5.0.
Yes, I want to restart my computer now.
No, I will restart my computer later.
A restart is required before VMS can be used.
< Back
Finish
Cancel

1.7. Starting the SCC Client

To start the software, click **Programs > SCC Suite > SCC** under the Windows **Start** menu.

The software will prompt for the following information:



- **Access Method** – Directly Access or Internet Port Forward.
- **Type** - Choose SCC.
- **Server** – The IP address for the SCC/NVR Server. You can click **Search** button to obtain it. For users of port forwarding, it should be the IP address of the router.
- **Port** - The Login Port for port forwarding - 9050. It should be set under ***Server > Other Tasks > Port Mapping*** after the first login.

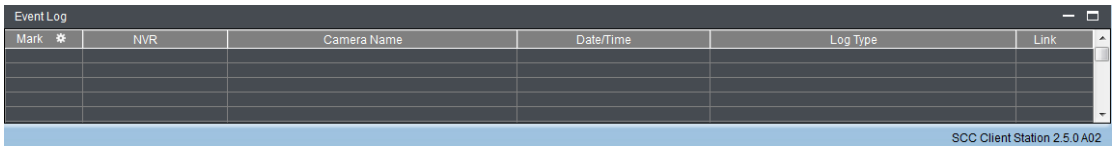
Note: (1) Please refer to *Port Forwarding Section* for more details.

- **Username** – The username for the domain, **which is always *admin*.**
- **Password** – The password for the domain. **Default password is *admin*.**

Click **Login** after the password (and port number) is entered.

1.7.1. Checking the Software Version

Users can see the software version at the lower right corner of the window after logging in.



1.7.2. Logging out

The Client can be logged out of all the Servers configured on the system by pressing the **Logout** button on the upper right hand corner in the GUI. Logging out of individual servers can be achieved by double clicking the server entry and clicking the **Yes** button on the confirmation screen.

Closing the window using the **X** button on the top right corner will exit the Client. A confirmation screen will appear, click **Yes** to exit the system.

Note: (1) If the system becomes unresponsive, users can force shutdown the system (press and hold the power until the system shuts down). This should only be done when the system is unresponsive!

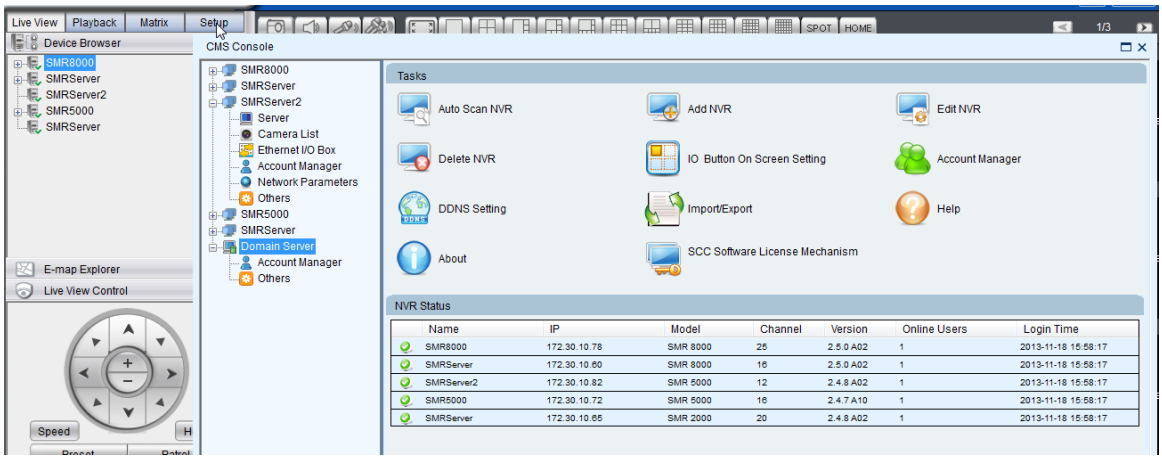
Chapter 2. Basic System Settings

2.1. Adding NVRs to the Server

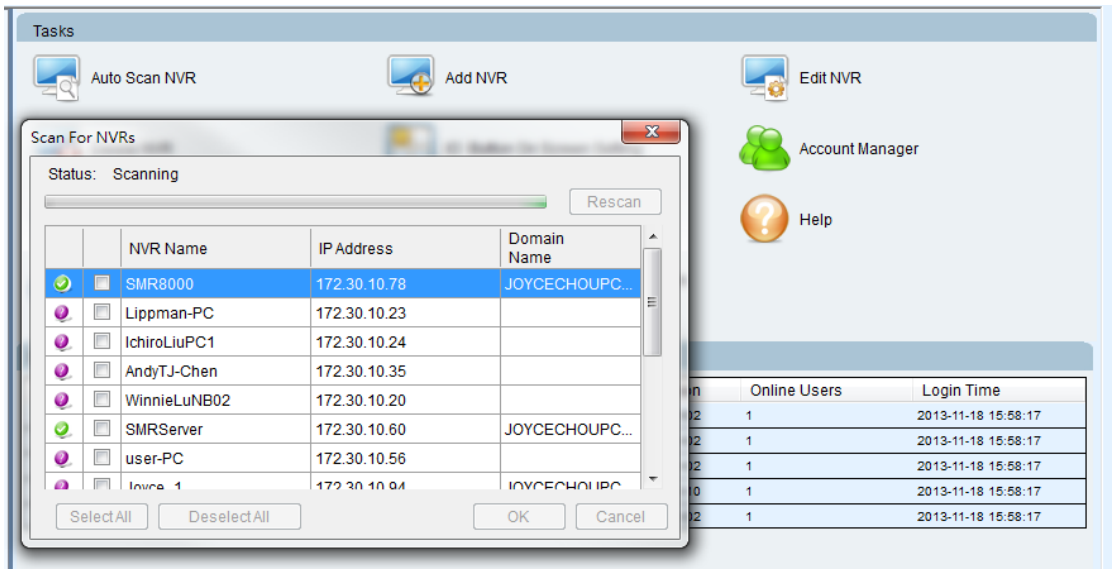
NVRs can be added to the Server in two ways: via an automatic scan or by manually inputting the NVR information.

2.1.1. Automatic Scan for NVRs

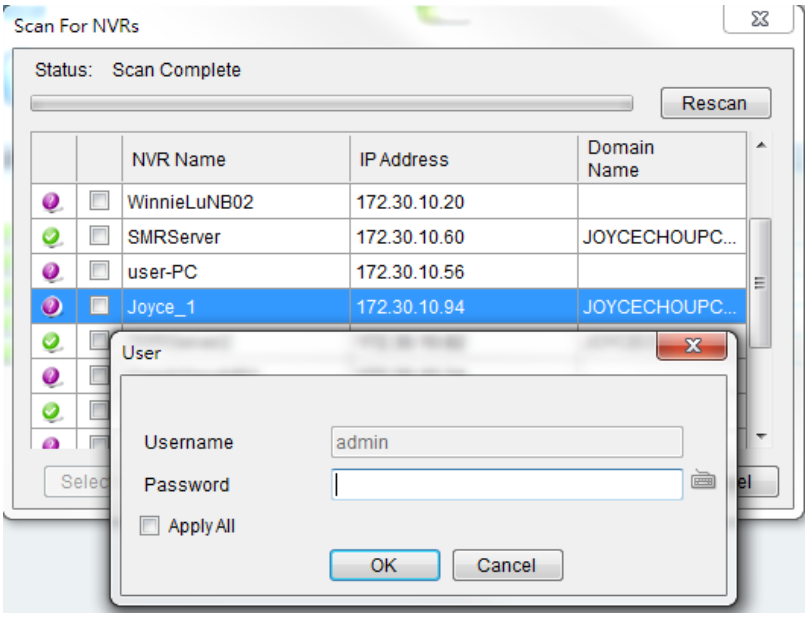
1. Go to Setup page and select Domain Server to see the following image.



2. Click on the first option “Auto Scan NVR”, it will start auto scan available NVRs as the shown image below.

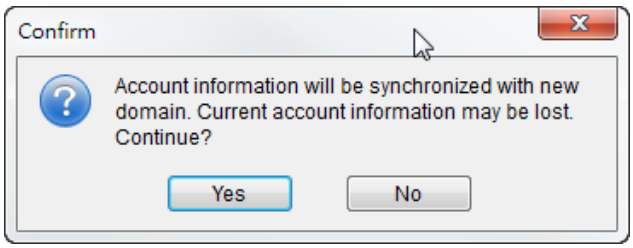


3. Check the server you'd like to add on the list and it will prompt a dialogue asking for the Password of the selected server.

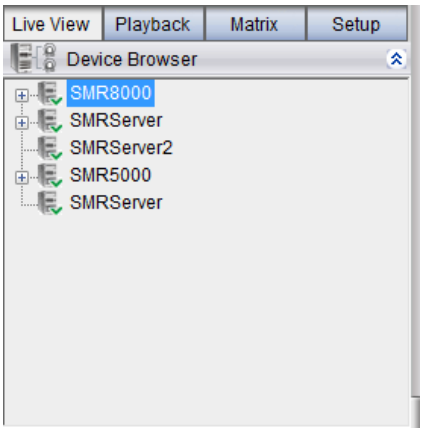


4. After inputting the Password, click OK and a notice will show up, warning you that Account information will be synchronized with new domain. Current account information may be lost.

   Once confirmed, click Yes.

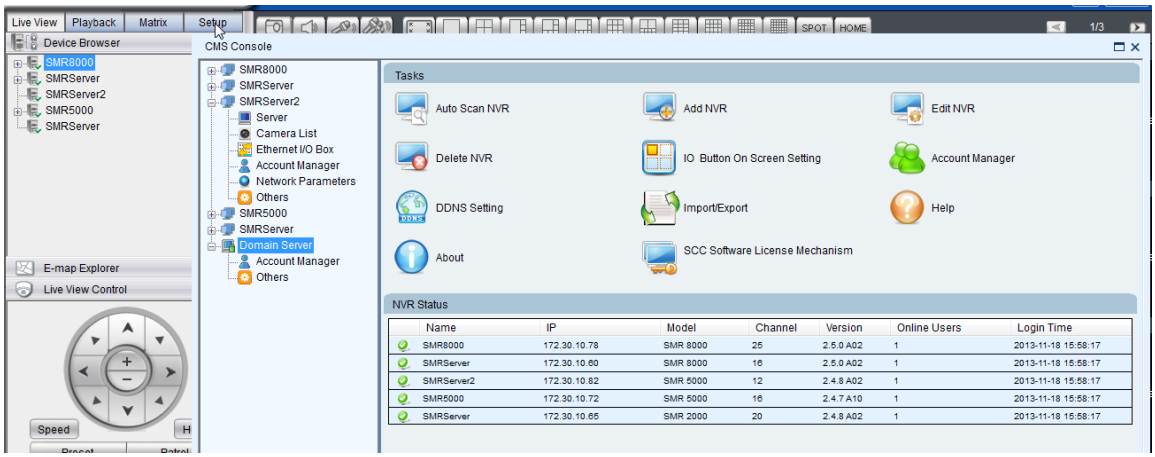

Confirm
Account information will be synchronized with new domain. Current account information may be lost. Continue?
Yes
No

The selected server will be added in the Device Browser on the left of page.

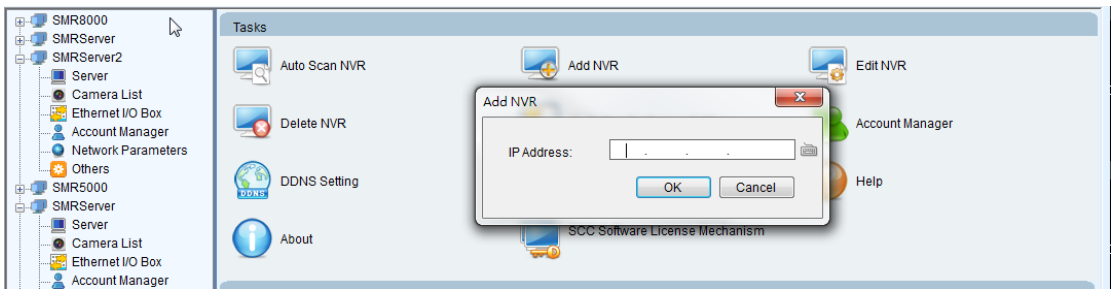


2.1.2. Manually adding NVRs

1. Go to Setup page and select Domain Server to see the following image.

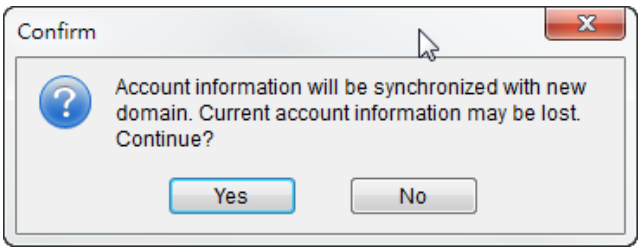


2. Click on the second option “Add NVR”, it will prompt a page for you to input the IP Address of the server you’d like to add in.

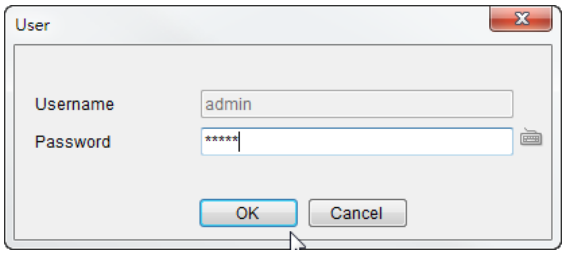


3. After inputting the IP Address, click OK and a notice will show up, warning you that Account information will be synchronized with new domain. Current account information may be lost.

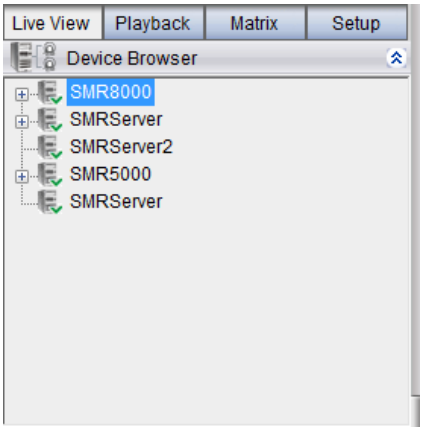
Once confirmed, click Yes.


Confirm
Account information will be synchronized with new domain. Current account information may be lost. Continue?
Yes
No

4. After clicking yes, it will prompt a dialogue asking for the Password of the selected server.



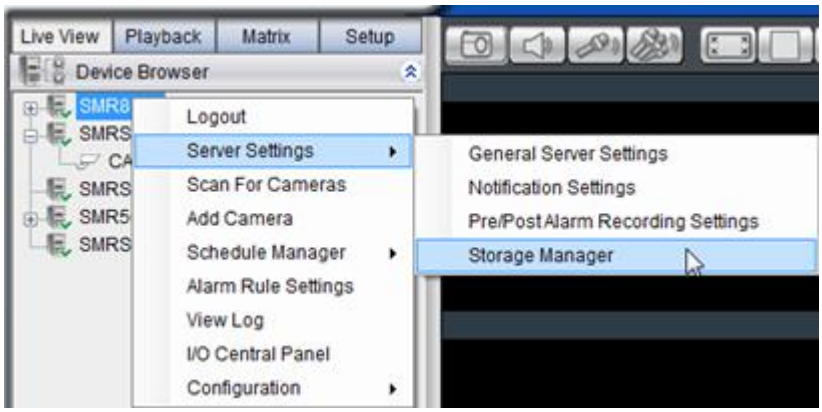
The selected server will be added in the Device Browser on the left of page.



2.2. Storage Management

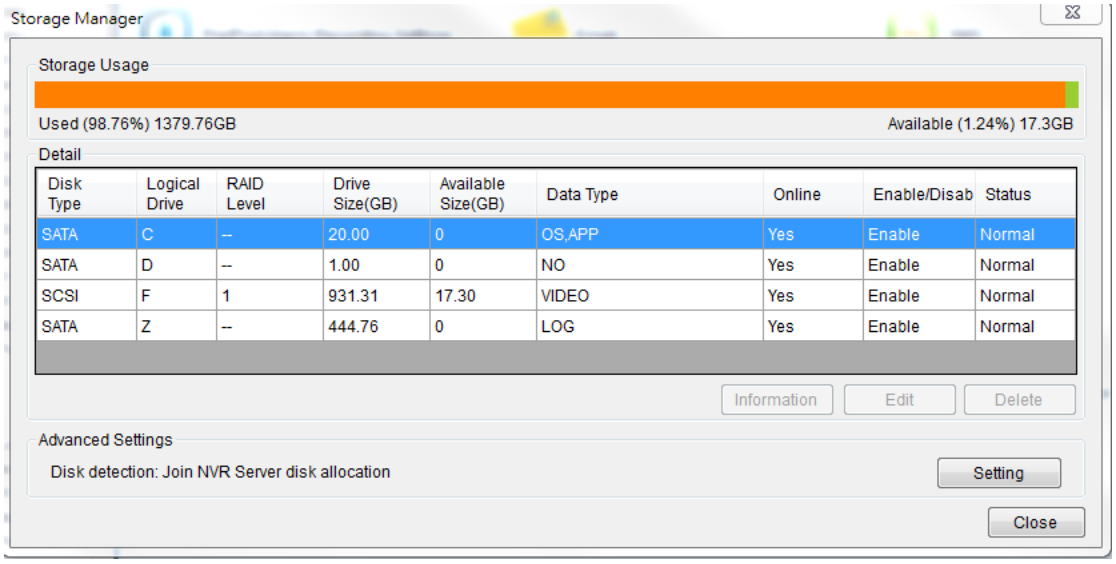
1. To access the information about the drives configured in your NVR/SMR, highlight and click the **Storage Manager** option under **Server Settings**.

If this process is done before connecting to SCC, you can skip the storage management option.



2. All available Logical Drives, as well as their sizes, free space, and status will appear.

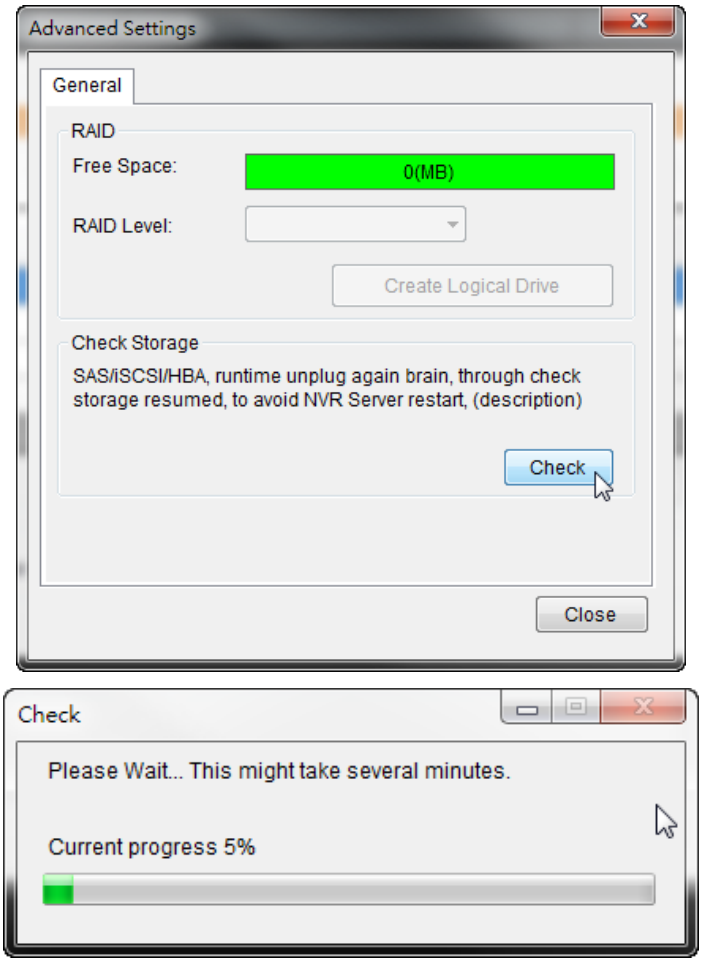
Click **Edit** to set the log and location for saving the video recordings.


Storage Manager
Storage Usage
Used (98.76%) 1379.76GB
Available (1.24%) 17.3GB
Detail
Disk Type | Logical Drive | RAID Level | Drive Size(GB) | Available Size(GB) | Data Type | Online | Enable/Disab | Status
SATA | C | -- | 20.00 | 0 | OS,APP | Yes | Enable | Normal
SATA | D | -- | 1.00 | 0 | NO | Yes | Enable | Normal
SCSI | F | 1 | 931.31 | 17.30 | VIDEO | Yes | Enable | Normal
SATA | Z | -- | 444.76 | 0 | LOG | Yes | Enable | Normal
Information
Edit
Delete
Advanced Settings
Disk detection: Join NVR Server disk allocation
Setting
Close

(Step 3 and 4 are for the remote client of NVR2000/SMR Series.)

3. Click the target drive first and then **Settings**.

   In “Advanced Settings” dialogue, “General” tab, click **Check**.



4. Choose the RAID level, and then click **Create Logical Drive** to create the RAID configuration.

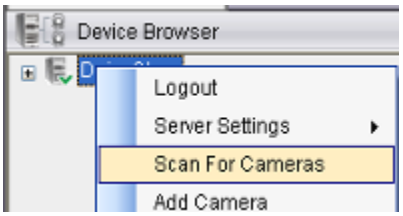
Note: Storage Manager can also be accessed by clicking ***Server*** > ***General Tasks*** > ***Storage*** *or* ***Server Entry*** > ***Common Tasks*** > ***Common Server Tasks*** > ***Storage*** in the SCC Console.

2.3. Adding Cameras to the Server

Cameras can be added to the Server in two ways: via an automatic scan or by manually inputting the camera information.

2.3.1. Automatic Scan for Cameras

To begin an automatic scan for cameras:



1. Right-click the Server entry and select **Scan for Cameras**. The system will respond by beginning an automatic scan. Once the scan is complete, the cameras that can be added to the Server will be displayed. Information available for each camera will include:

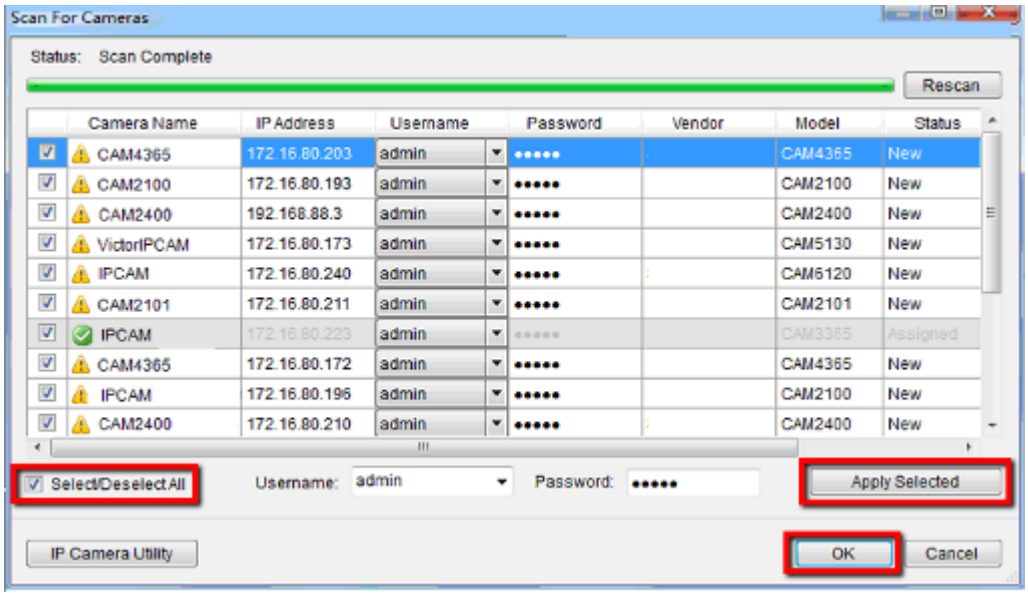
    - **Name** – The default camera name (Make/Model)
    - **Status** – The camera will display *New* if it has not been added to this Server, otherwise it will display *Assigned*.
    - **IP Address**
    - **MAC Address**

    - **Vendor - Including ACTI, ASONI, AVTECH, AXIS, Arecont, Sosch, Brickcom, DyNACOLOR, D_Link, Dahua, EDIMAXHIKVISION, EverFocus, HIKVISION, IQinVision, Lilin, Eessoa, Mobotix, ONVIF, Panasonic, SIMON, SONY, Samsung, Surveon, VIVOTEK, and General.**

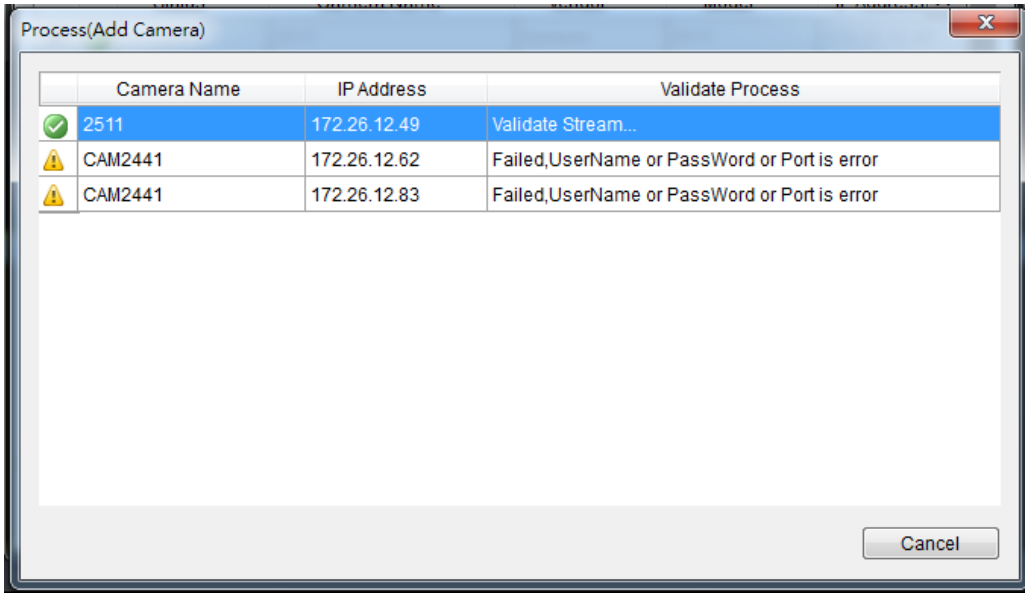
    - **Model -** when **"General"** is selected, **"RTP over TCP"** and **"RTP over UDP"** can be further defined.

2. To add a camera to the system, check the box by the camera entry. You may also check the **Select All** box at the bottom of the window to select all the cameras found.

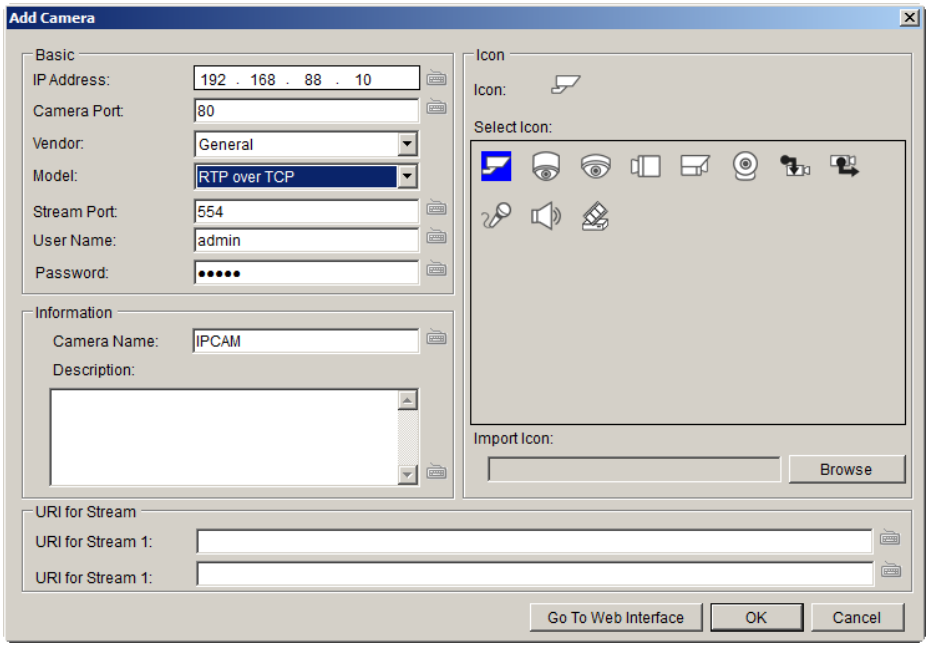
Enter the username and password, and press **Apply Selected**. Click **OK** to add the selected cameras to the Server.



The following windows will prompt for validation.



3. **(Optionally)** Double-click any camera entry to bring up the camera detail page. From this page you may change the following information:



- **IP Address** – Changing this value will affect connectivity.
- **Camera Port -** The web access port, default is 80.
- **Stream Port** – Default is 6002.
- **Vendor** – Changing this value will affect connectivity.
- **Model** – Changing this value will affect connectivity.
- **User Name** – This value is not always required.
- **Password** – This value is not always required.
- **Camera Name** – It is recommended you change this value if you have more than one camera of this make/model.
- **Camera Description**
- **Camera Icon -** You can also import your own icon by clicking on the **Browse** button and choosing an icon file. Valid icon files include JPEG, GIF, PNG, BMP and ICON files.

Finally, you can access the web interface for the camera by clicking on the **Go to Web Interface** button. Click **OK** to save your changes, or **Cancel** to exit without saving.

4. **(Optionally)** You may access the IP Utility for camera configurations by clicking the **IP Camera Utility** button.

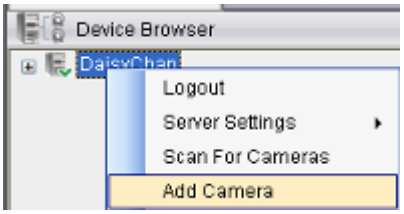
5. Click **OK** to add the selected cameras to the Server.

Note: Automatic Scan for Cameras can also be accessed by clicking ***Camera List*** > ***General Tasks*** > ***Scan for Cameras*** *or* ***Server Entry*** > ***Common Tasks*** > ***Common Server Tasks*** > ***Scan for Cameras*** in the SCC Console.

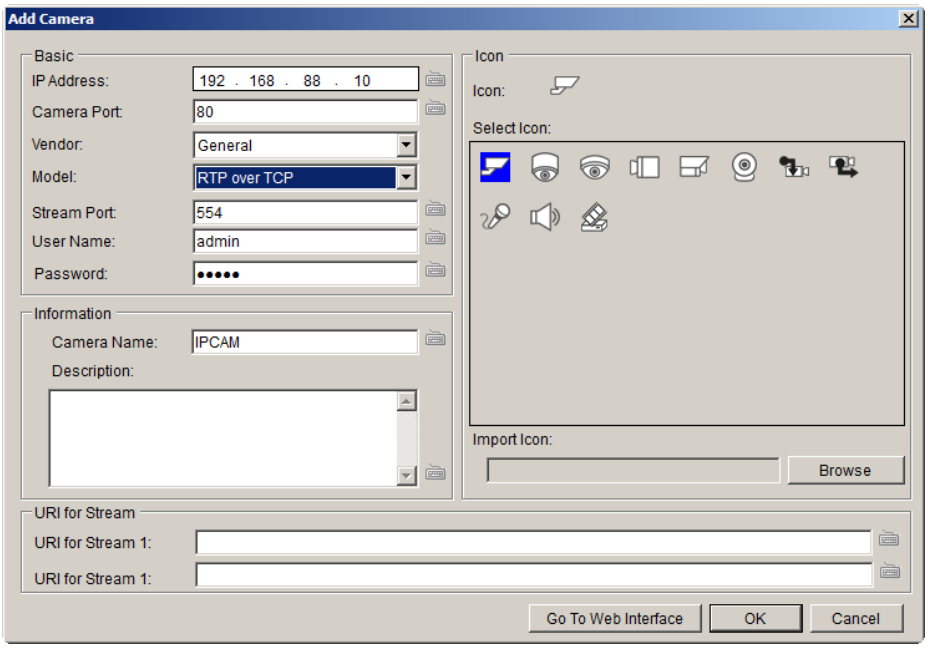
2.3.2. Manually Adding Cameras

To manually add a camera to the Server:

1. Right-click the Server entry and select **Add Camera**.



2. In the camera window fill out the following information:



- **IP Address**
- **Camera Port** - This value will automatically populate with the default value for the **Vendor** and **Model** selected.
- **Vendor - Including ACTI, ASONI, AVTECH, AXIS, Arecont, Sosch, Brickcom, DyNACOLOR, D_Link, Dahua, EDIMAXHIKVISION, EverFocus, HIKVISION, IQinVision, Lilin, Eessoa, Mobotix, ONVIF, Panasonic, SIMON, SONY, Samsung, Surveon, VIVOTEK, and General.**

- **Model -** when **"General"** is selected, **"RTP over TCP"** and **"RTP over UDP"** can be further defined.
- **Stream Port -** This value will automatically populate with the default value for the **Vendor** and **Model** selected.
- **User Name** – This value is not always required.
- **Password** – This value is not always required.
- **Camera Name** – It is recommended you change this value if you have more than one camera of this make/model.
- **Description**
- **URI for Stream:** when **"General"** is selected, **"URI for Stream 1"** can be further defined.

  For example:

  For a Surveon IP camera, type
  RTSP://<IP of the IP camera>/stream1 or stream2

  For an AXIS IP camera, type
  RTSP://<IP of the IP camera>/<codec>/media.amp

  For a HIKVISION IP camera, type
  RTSP://username:password@<IP of the IP Camera>

- **Import Icon -** You can also import your own icon by clicking on the **Browse** button and choosing an icon file. Valid icon files include JPEG, GIF, PNG, BMP and ICON files.

3. Finally, once basic camera information is filled in, you may access the web interface for the camera by clicking on the **Go to Web Interface** button. Click **OK** to add the camera.

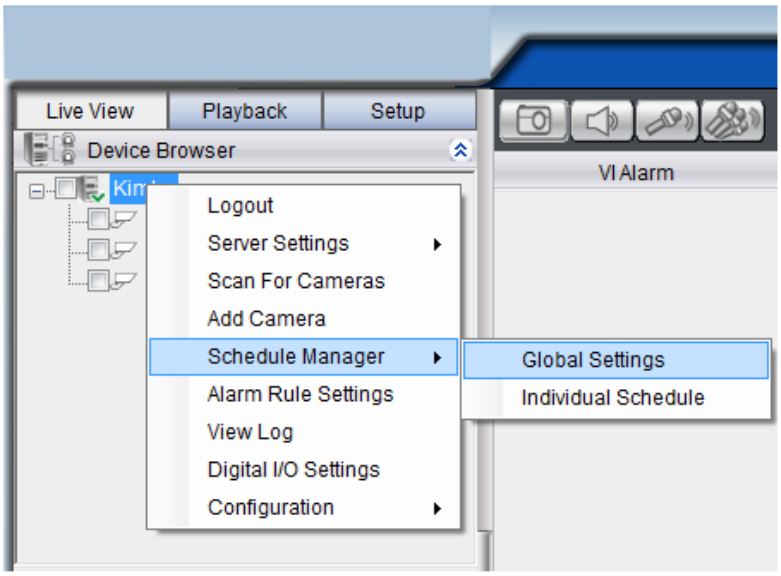
Note: Cameras can also be added manually by clicking ***Camera List > General Tasks > Add Camera*** in the SCC Console.

2.4. Setting Recording Schedule

A global Schedule applies to all cameras, while individual schedules are for each camera. Individual schedules take precedence over global schedules.

2.4.1. Weekly Scheduling

1. Right-Click the SCC entry and choose **Schedule Manager > Global Settings** or **Individual Schedule** to bring up the Weekly Schedule popup.

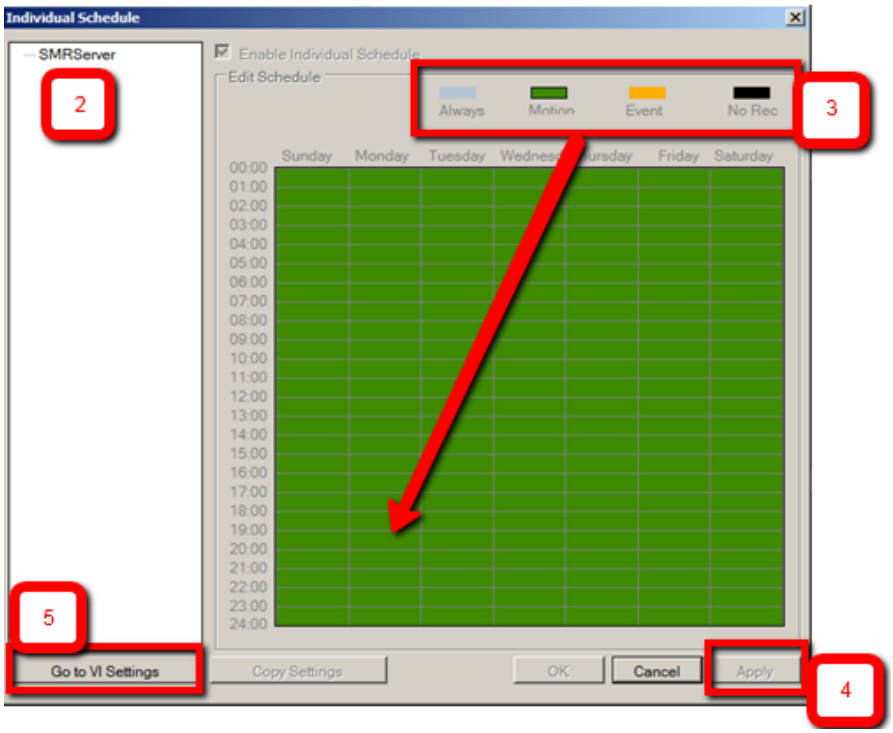


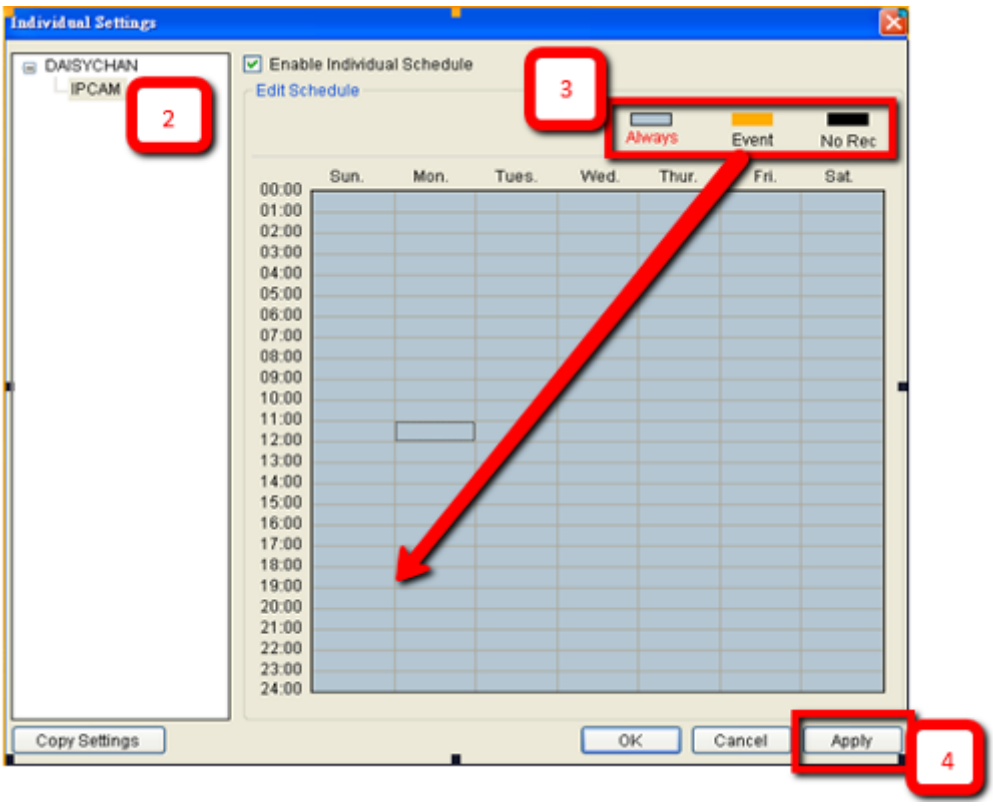
2. If setting individual schedule and more than one camera is configured, choose the camera you wish to set from the list.

3. The schedule grid corresponds to every hour in the week. Click on one of the four recording methods and then click on the grid area to “paint in” the method for the corresponding hour.

4. Click the **Apply** button to apply the schedule and **OK** to exit the dialog.

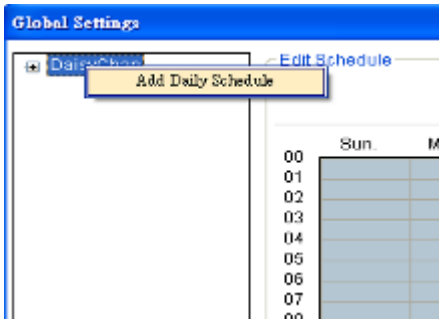
5. **(Optional)** You may go to the VI setting panel by clicking **Go to VI Settings.**



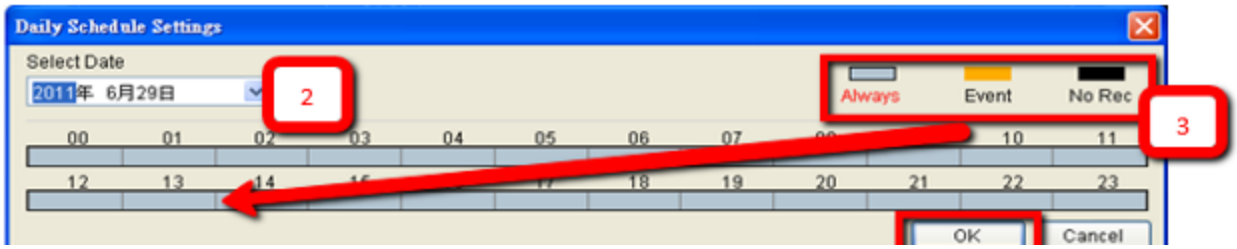


2.4.2. Daily Scheduling

1. Right Click the server entry and choose **Add Daily Schedule**.



2. Click the **Select Date** selection box and choose the date that you want to schedule.



3. Click on one of the methods and then click on the grid area to “paint in” the method for the corresponding hour.

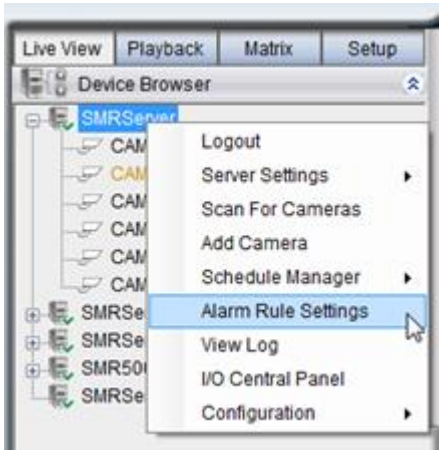
4. Click **OK** to apply the changes.

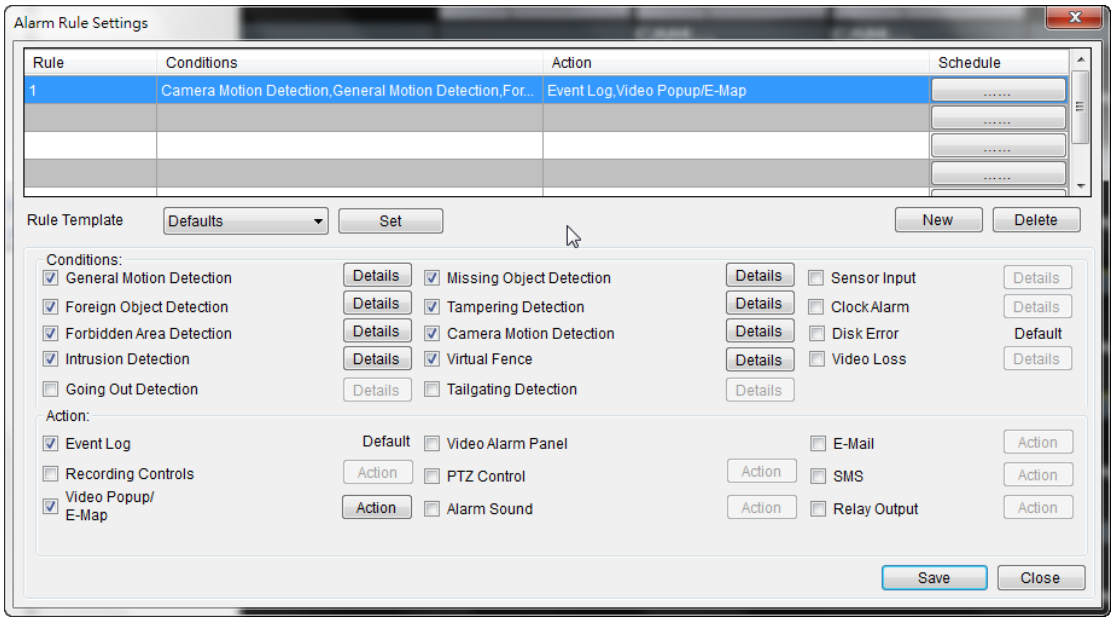
2.5. Adding Alarm Rules

Alarm rules can be created using the following elements:

- **Rule**: A short description. For example, “east-fence intrusion detection” or “front entrance access control.”
- **Condition**: Specifies triggering conditions such as Motion/Video loss/Sensor input/Clock Alarm, etc.
- **Action**: Specifies the action to take when the alarm is triggered.
- **Schedule**: Allows the user to schedule the application of specific Alarm rules. This is useful in cases such as applying rules to non-office hours.

1. Right-click the NVR entry and select the **Alarm Rule Settings** option under SCC node.



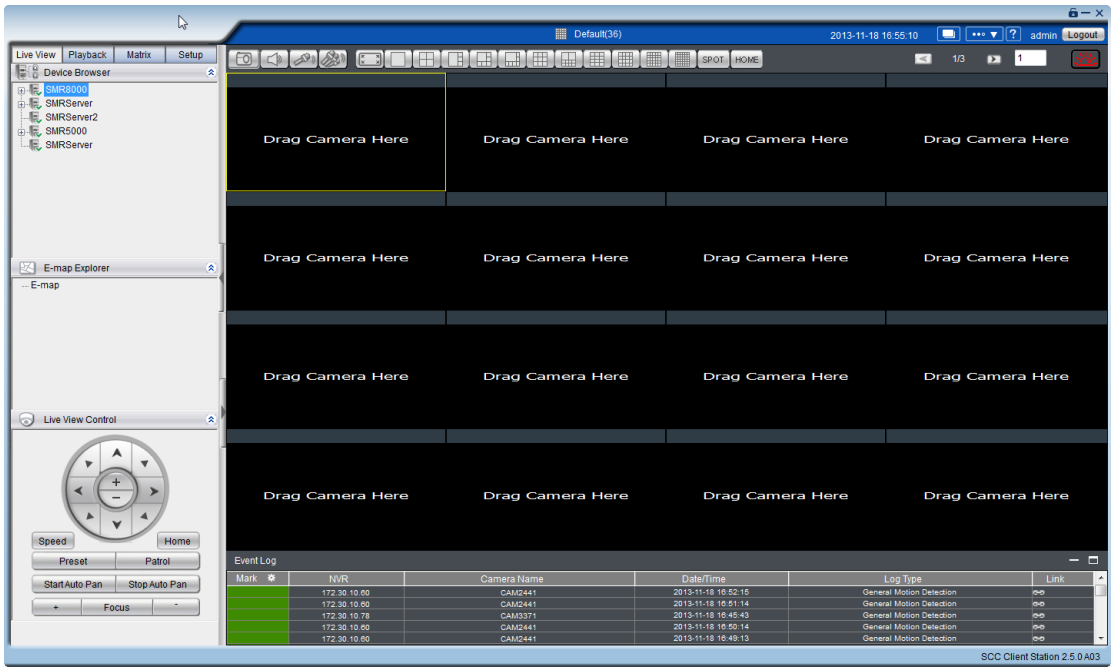


2. Click the **New** button.
3. Enter name for the new rule and click **OK** to create the rule.
4. Choose conditions for the Alarm. Detailed settings can be changed by clicking **Details.**
5. Select actions for the alarm. Detailed settings for actions can be set by clicking **Action.**
6. Click the……button in the alarm field to set up a schedule for the rule. Default scheduling is record always on.
7. Click the **Save** button to save the rule.

2.6. Setting up Live View

An important part of monitoring your surveillance network is to have the right views so that you will have the optimum viewing angle to discern a situation.

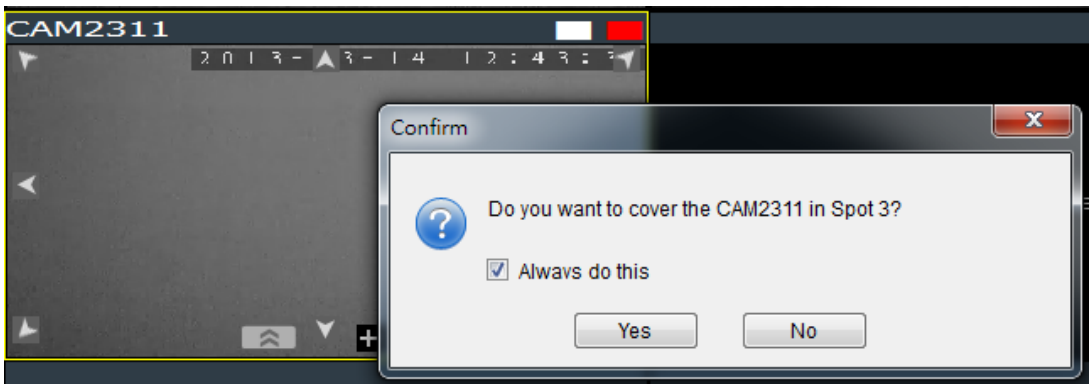
The default view setting is 3x3.



You can also add a customized view to the SCC Client:

1. Right click on **Views > Add View** in the *View Explorer* window of the SCC, and choose the type of view that you wish to add. The software responds by placing a blank template in the main viewing area.
2. From the *Device Browser* window, you can click and drag each camera into separate frames. The camera output will be displayed in the frame.

When two cameras are dragged into the same view, a popup window will ask you whether you want to use the latter camera to replace the former one.

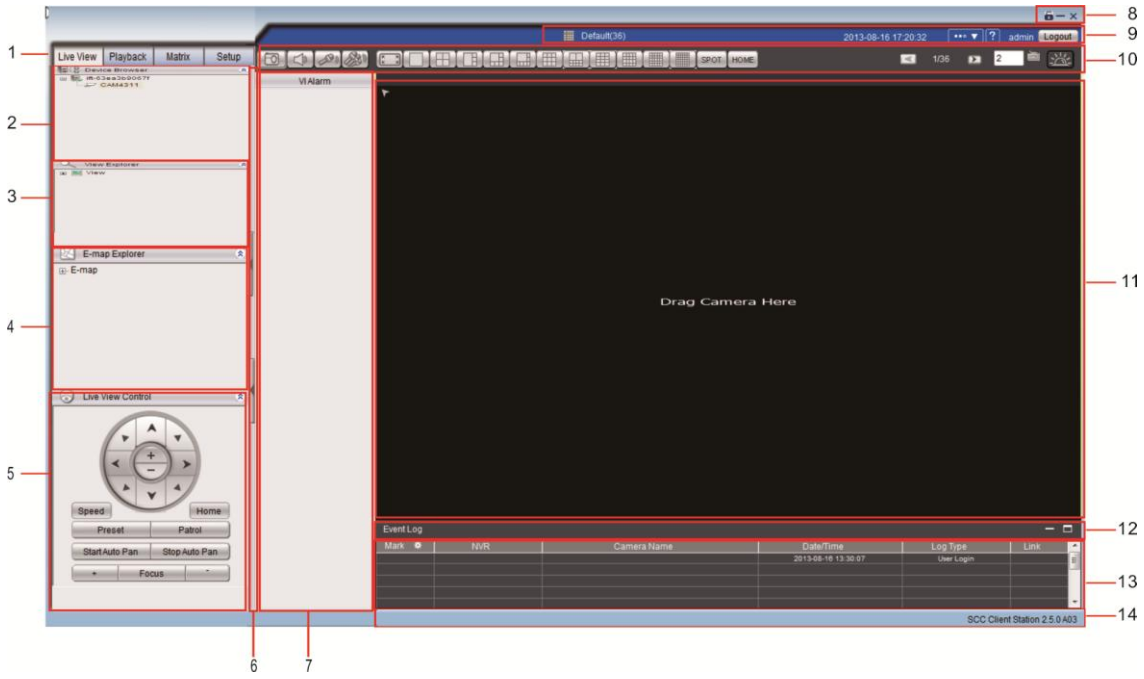


Chapter 3. Live View

Live viewing is a crucial part of any surveillance system. Having the right view can be the crucial difference between catching an event as it happens and missing it altogether. SCC provides powerful tools to manage the viewing experience to help ensure that monitoring personnel are always on top of any event.

3.1. Live View Window Overview

The live view window is split into 14 distinct parts:



1. **Live View / Playback / Matrix / Setup Selection Tabs** – Allows users to choose live view, playback and matrix mode.
2. **Device Browser** – Lists the Servers in the domain.
3. **View Explorer** – Lists the views that are configured on this client.
4. **E-Map Explorer** – Lists the E-maps available on this Server.
5. **Live View Control** – Interface for interacting with PTZ-enabled cameras.

6. **Arrows for open up or close in the image panel and the VI Alarm panel.**
7. **VI Alarm** –Area for alarm notification and instant playback.
8. **Window Toolbar** – Lock the window, minimize the window, or leave the system.
9. **View/Account Information** – This area contains general information. Arrow button containing Server configuration options. Question mark indicates Help File. Logout button for a quick logout.
10. **Button Area** - This area contains the buttons to change views, enter full screen mode, capture photos, send audio files to the chosen / all cameras and other useful functions.

	Snapshot
	Volume control
	Talk to the chosen camera
	Broadcast to all the cameras
	Full screen mode
	Viewing screen modes
	Auto page flip between pages
	Reset all the settings, including page auto-flipping and different screen divisions

11. **Main View Area** – This area contains the actual video feed(s).
12. **Event Log Window** – Close or send to another window for a better view of the Event Log.
13. **Event Log** - This area contains alarm and event information.
14. **Version** – Shows the current SCC version.

3.1.1. Resizing and Minimizing Windows

Minimizing Controls

The Device Browser, View Explorer, E-Map Explorer, Live View Control, Matrix Slave, and Event Log can all be minimized by clicking on the arrow buttons on the top-right corner of their screens.

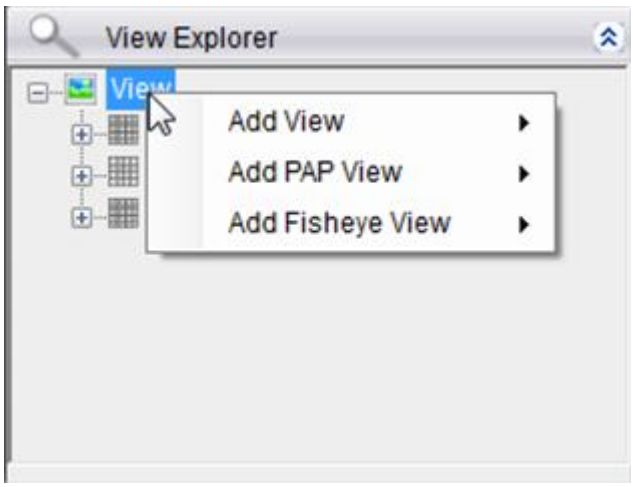
Hiding and Showing the Explorer Area

The entire left panel (containing the Live View / Playback / Matrix Selection Tabs, Device Browser, E-Map Explorer, View Explorer and Live View Controls) can be hidden by clicking on the arrow on the left of the Live View Control.

3.2. View Setup

3.2.1. Types of Views

The SCC/NVR server supports viewing of up to 32 cameras in a single view, with views of up to 36 cameras.

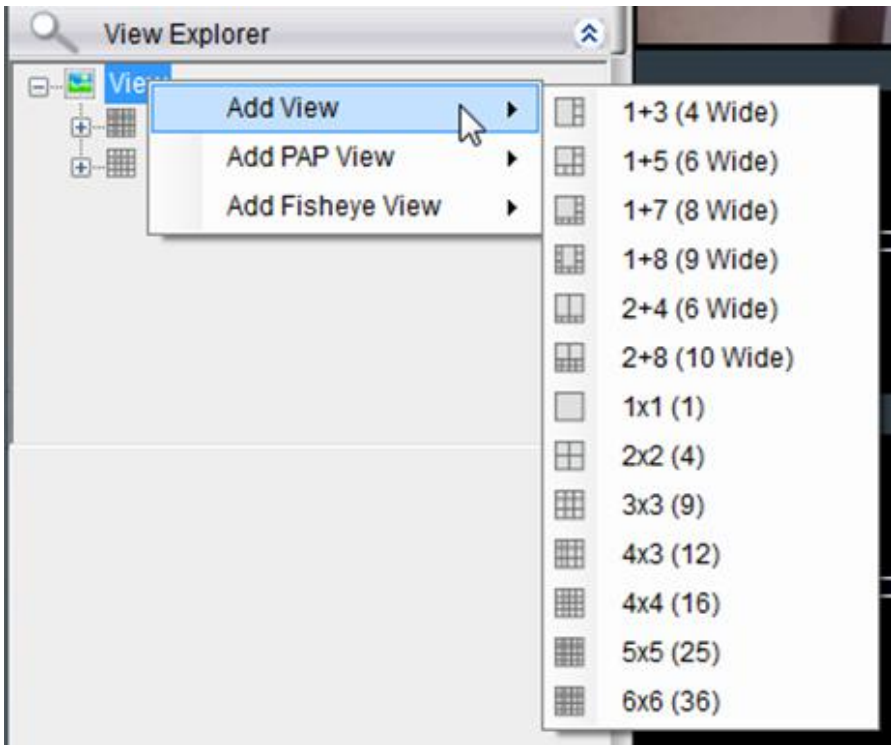


Note: SMR2000/5000 series supports views of up to 16 cameras.

Views with more subdivisions are more useful for giving an overview of an area, while ones with fewer subdivisions give better details. Multiple views can also be displayed in sequence or in separate windows for managing more than 16 cameras.

3.2.2. Add View

An important part of monitoring your surveillance network is to have the right views so that you will have the optimum viewing angle to discern a situation. To add a customized view to the SCC client:



1. Right click on **View** in the *View Explorer* window, and choose the **Add View** option, the software will respond by listing available screen division types.
2. Choose the type of view that you wish to add by clicking on the view. The software responds by placing a blank template in the main viewing window that has been subdivided into individual frames according to the view selected. The empty frames will display the message *No camera*.
3. From the *Device Browser* window, you can click and drag the entries for individual cameras into the separate frames. The camera output will be displayed in the frame. Cameras in the view do not have to all be from the same server.

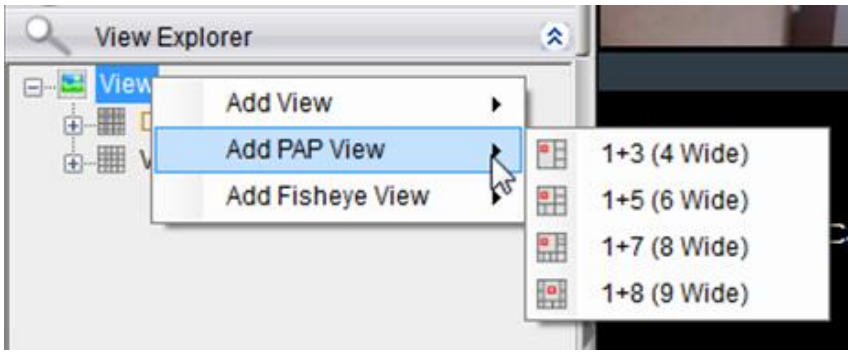
Dragging a camera into a frame that already has a camera assigned to it will cause the frame to be reassigned to the new camera. You can also drag the same camera into multiple frames or leave frames blank, although this is not suggested.

The *View Explorer* will be updated as you add cameras to your view. The root will list the camera numbers that have been added to the view starting from the top left frame and going from left to right and top to bottom.

> **Note:** Depending on your connection and computer speed, it may take a moment for the image to refresh after dragging the camera into the view window. During this time the frame may still display *No Camera* or *Failed to connect*. If this problem persists, however, there may be a problem with your connection or hardware.

3.2.3. Add PAP View

PAP (Picture and Picture) View allows you to select multiple regions from one image to zoom.

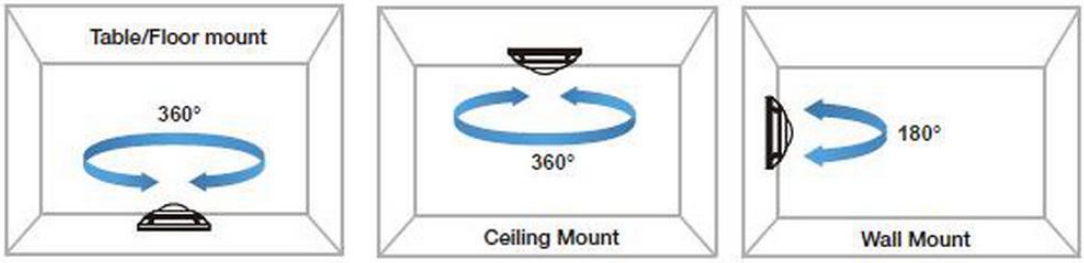


1. Right-click the **View** entry in the View Explorer window. This will bring up an options popup.
2. Select "Add PAP View" and then select the desired window number. 1 indicates the main original image and the number behind "+" means the numbers of the zoomed areas that you are about to create. For example, 1+8 means 1 main original image + 8 zoomed areas.
3. Drag the set value from the View Explorer to the main image window.
4. Drag the desired camera from the Device Browser to the main image window. Images from the camera you dragged will appear on the main image window.
5. Move your mouse to select one window from the zoomed windows on the right. From the main image window use your mouse to drag out an area you'd like to zoom for the selected zoomed window. Zoomed images will appear on the zoomed windows.

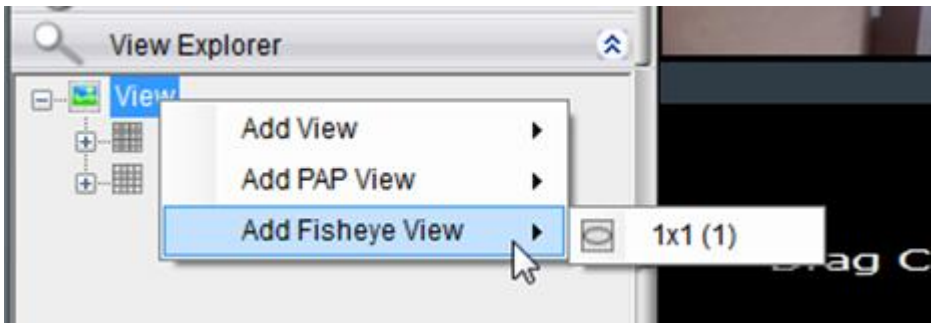
6. Repeat Step 5 to create more zoomed areas; 8 zoomed areas can be created when you set the PAP view to 1+8.
7. Move the cursor to the box of the unwanted region and left click to see the options, Clear Region (clear 1 selected region)/ Clear All (clear every created region).

3.2.4. Add Fisheye View

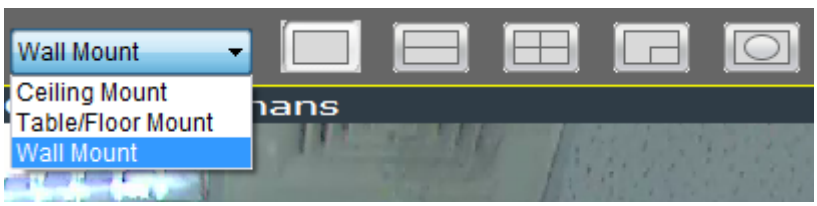
Viewing angles are crucial for fisheye cameras to capture images and different installation method can affect the viewing angles. Fisheye viewing is supported in SCC.



1. Right-click the **View** entry in the View Explorer window. This will bring up an options popup.
2. Select "Add Fisheye View" and then "1x1(1)".



3. Drag the desired camera from the Device Browser to the main window. Images from the camera you dragged will appear on the main image window.
4. Select according to the way your fisheye is installed to have a best viewing result, Ceiling Mount, Table/Floor Mount or Wall Mount.



5. The distorted hemispherical image of the fisheye camera can be converted into a conventional rectilinear projection , a split-window , a 4 split-window , and the original fisheye view .

3.2.5. Renaming a View

To perform this function:

1. Right-click the view entry in the *View Explorer* window. This will bring up an options popup.
2. Highlight and click the **Rename** option.
3. Enter a new name for the server and press enter to save the name.

3.2.6. Deleting a View

As views become superfluous or unused, it is desirable to delete a view. To perform this function:

1. Right-click the view entry in the *View Explorer* window. This will bring up an options popup.
2. Highlight and click the **Delete** option. The system will respond with a confirmation screen.
3. Click the **Yes** button to delete the view.

3.2.7. Sending View to a New Window

In multi-monitor setups, you may send views to a separate window which can then be dragged to other screens. To do this:

1. Right-click the view entry in the *View Explorer* window. This will bring up an options popup.
2. Highlight and click the **Send View To > Floating Window** option. The system will respond by placing the view in a separate floating window. This window can be dragged to a separate screen, maximized, or closed.

3.2.8. Switching Between Views

To switch between saved views, simply click and drag the view entry from the *View Explorer* window into the main view window. Note that the current view is always indicated in **Bold** lettering in the *View Explorer* window.

3.2.9. Switching Between Different Screen Divisions

Creating and Using New Screen Divisions

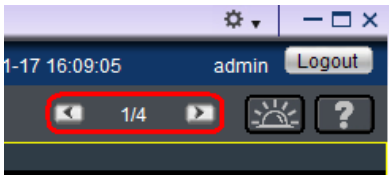
When a view is created, it has a default screen division setting, however when using the view, it may be useful to change the number of screen divisions. This does not create a different view, but divides the existing view into a new set of divisions.

To perform this function within the view, simply click the button corresponding to the view that you want to use. The buttons are located in the area above the main view window.

After you have clicked on the desired view, the original number of cameras will be split into separate pages in the new view. For example, an original view consisting of 16 cameras would display the cameras on 2 pages of 8 frames, clicking on the 4 division button would display the 16 cameras in 4 pages of 4 frames each.

Screen Division Page Use

The page number is displayed to the right of the view buttons. Clicking on the arrow button to the right of the page number or clicking on the current screen partition button will scroll through the pages in order. Clicking on the arrow button to the left of the page number will scroll through the pages in reverse order.

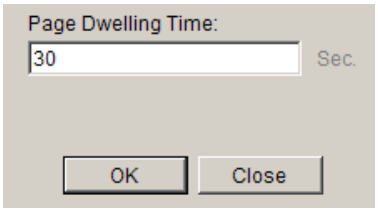


Auto-flipping Pages

When multiple pages of screen divisions exist, you may choose to automatically flip between the pages by clicking on the **SPOT** button. Clicking the button again will end the automatic flip function.

Configuring Page Dwell Time

Right-clicking the **SPOT** button will bring up a field to configure the amount of time each page will be displayed when automatically flipping pages. Enter the dwell time in seconds and click **OK** to change this value.



Exiting Different Screen Divisions

There are two methods to return to your original un-paginated view. You may either drag the original view into the main view area, or click the **Home** button in the button area. This will reset all the settings, including page auto-flipping and different screen divisions.

3.3. Functionality Within Views

Right clicking an active window will cause a function list to appear. These are settings and functions that can be changed within the live-view window.

3.3.1. Digital Zoom

Digital zoom increases the view size without increasing resolution. The digital zoom function can be used within any panel (even in full screen mode) with the following steps:

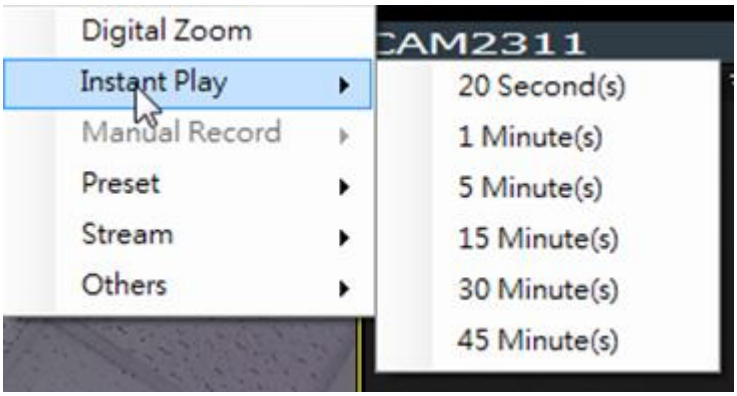
1. Right-click the panel that zoom is required on, and select **Digital Zoom** to activate the function. A picture-in-picture showing the whole screen framed by a yellow box will appear.

2. Click the corners of the box and drag to resize it over the area of interest. The main picture will show the digitally-zoomed output, while the picture and picture will display the entire view.

3. Alternatively, you may use the mouse scroll to zoom into the center of the image. Scrolling forward will zoom in, scrolling backward will zoom out.

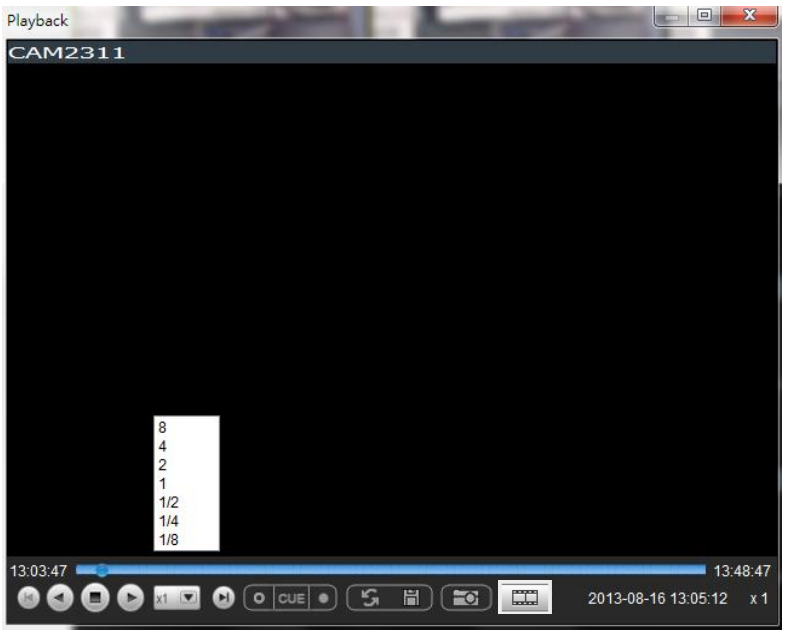
3.3.2. Instant Playback

The instant playback function gives users the ability to instantly playback up to 45 minutes of video. Right-click the video panel that playback is required on, and select **Instant Play > [Time Length]** to activate the function. A popup will open with the desired playback. Time lengths available are dependent on, and will not exceed the pre-alarm recording time set in Pre/Post Alarm Recording Settings.

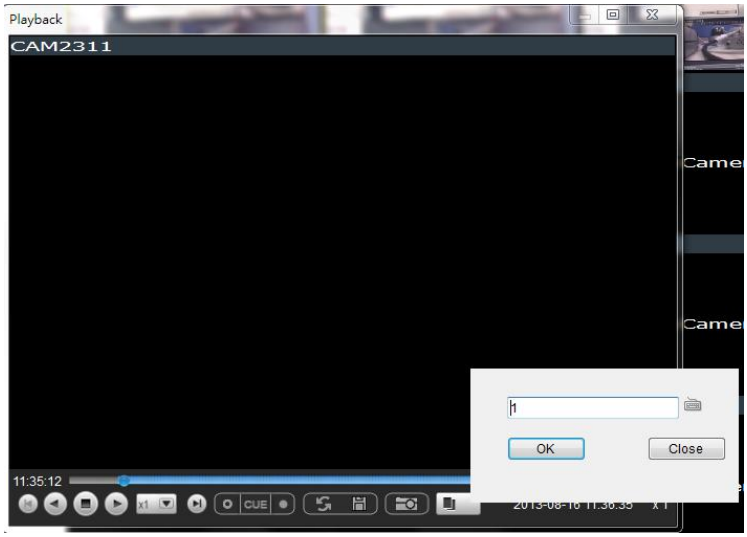


Playback can be displayed in 3 modes, Real Time , Frame By Frame , and Just Key Frame . The default setting is in Real Time Mode, clicking on the button to change modes.

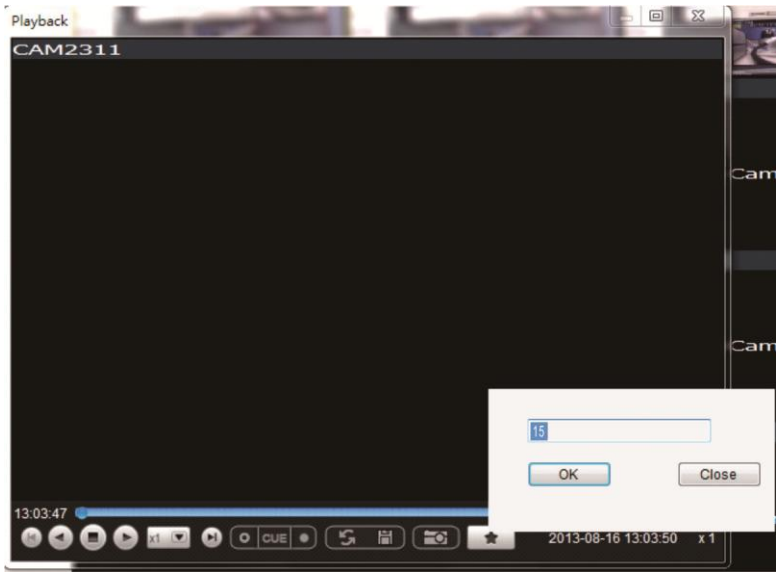
"Real Time" can be further defined to play in the speeds of 8x, 4x, 2x, 1x, 1/2x, 1/4x, and 1/8x.



“Frame By Frame” can be further defined to play in intervals from 1 to 15. Right click on the “Frame By Frame Mode” button to set the interval.



“Just Key Frame” can be further defined to play in intervals from 1 to 15. Right click on the “Just Key Frame Mode” button to set the interval.



The following table explains the buttons:

	Starts video playback.
	Reverses video playback.
	Stops video playback.
	Jumps to the next segment.
	Jumps to the previous segment.
	Clears the cue-in and cue-out markers.
	Set Cue-In marker for clip start
	Set Cue-Out marker for clip end
	Loop, continuous playback within Cue-In & Cue-Out
	Enable / Disenable loop. Loop to continuous playback within Cue-In & Cue-Out.
	Saves video clips/Exports selected clips.
	Snapshot
	Real time mode
	Frame by frame mode
	Just key frame mode

3.3.3. Manual Recording

When recording schedules are set, it may be necessary to manually record a video stream, even when the schedule does not specify for recording. In this case right-click the panel that recording is required on, and select **Manual Record > [5, 10 or 30 minutes]** to activate the function. The camera will record the stream for the amount of time specified.

3.3.4. Preset Pan

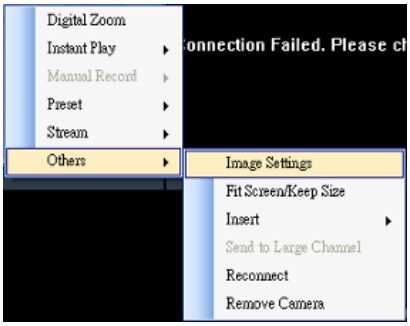
In cameras equipped with PTZ functionalities, presets set on the camera in the PTZ Preset Settings will be available. To access the presets, right-click on the panel containing the camera feed, and mouse-over **Preset**. The system will respond with a list of presets configured on the camera. Selecting a preset will pan the camera to the preset position.

3.3.5. Stream Selection

Video Streams can be selected by right-clicking the panel that playback is required on, and then select **Stream > Stream1/Stream2**.

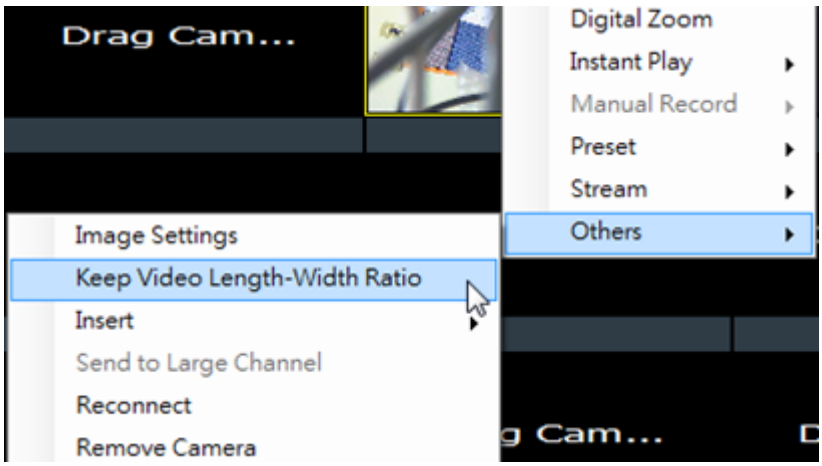
3.3.6. Image Settings

Camera image settings can also be accessed by right-clicking the panel containing the camera video and selecting **Others > Image Settings**. This will pull up the camera image settings menu.



3.3.7. Video Ratio Adjustment

In most cases the video panel size will not match the size of the video feed exactly. By default the SCC will stretch or shrink the video to fit the screen, however you may also choose to preserve the original video ratio by right-clicking the screen and selecting **Others > Keep Video Length-Width Ratio**. To return to a stretched view, right-click the appropriate panel and choose **Others > Resize to Fit Window**.



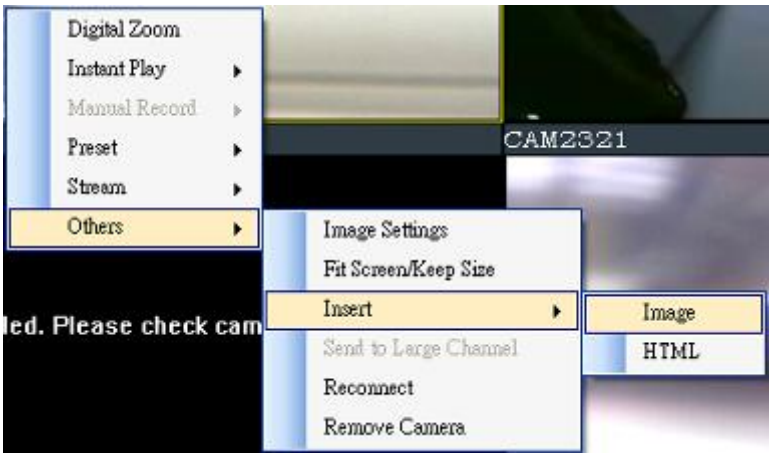
3.3.8. Inserting Overlays

The panel can be replaced with a user overlay.

Image Overlay

To overlay an image on top of a panel:

1. Right-click the panel and choose **Others > Insert > Image.** The system will prompt you to choose an image file.



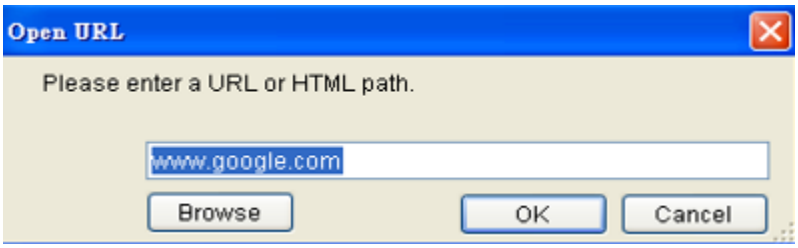
2. Choose an image file, valid image types are JPEG, BMP, TIF, PNG. Click **Open** to open the file.

3. The image will be displayed in the panel. Click the red X in the top-right corner to close the image.

HTML Overlay

The HTML overlay function allows simple integration of web applications in the SCC by replacing one or more panels of the screen with an active browsing window. To overlay an HTML form or website on top of a panel:

1. Right-click the panel and choose **Others > Insert > HTML**.



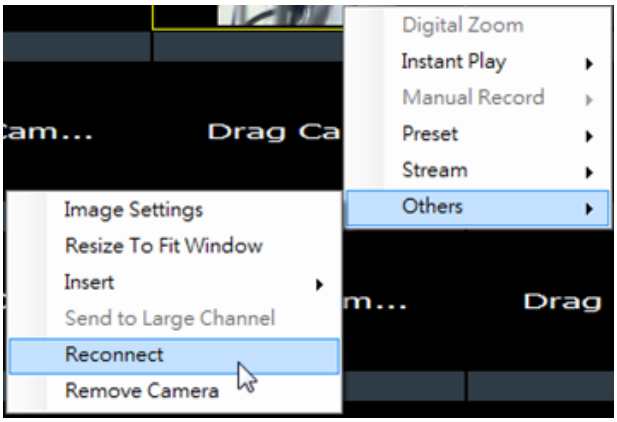
2. In the field, enter a URL or the path containing the HTML form. You may also choose to click **Browse** and choose an HTML file.
3. The HTML or website will be displayed in the panel. Click the red X in the top-right corner to close the image.

3.3.9. Send to Large Channel

Views in smaller divisions can be switched to the larger division. To perform this action, right-click the panel corresponding to the camera and choose **Others > Send to Large Channel.**

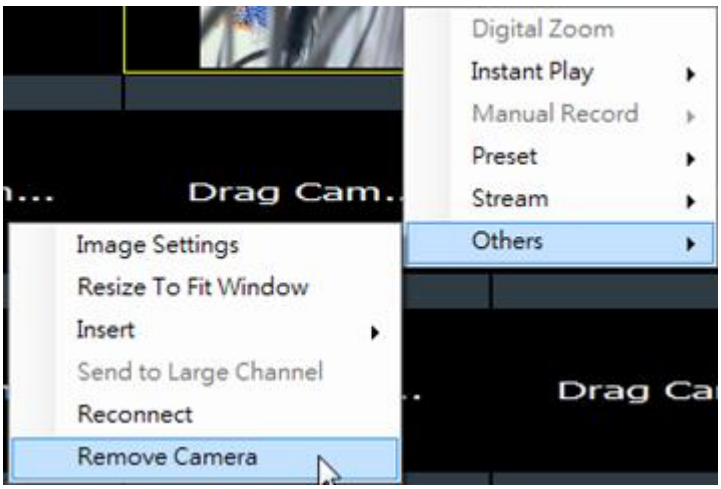
3.3.10. Reconnect

In some cases it may be necessary to manually reset the connection to a camera. To perform this action, right-click the panel corresponding to the camera and choose **Others > Reconnect.**



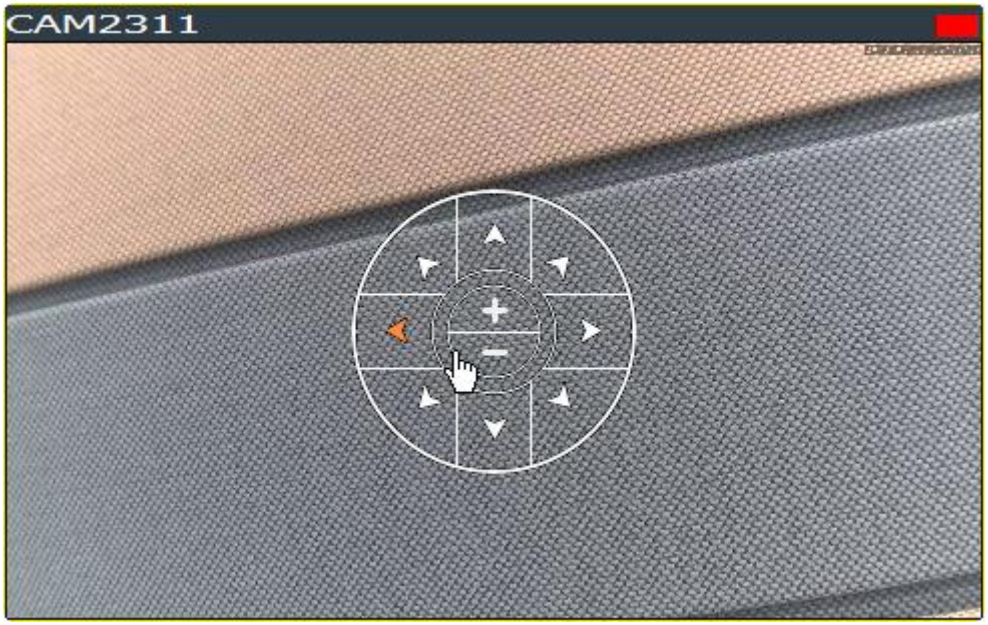
3.3.11. Remove the Camera

The Cameras can be removed by clicking **Others > Remove Camera**.



3.3.12. Onscreen PTZ Control

Cameras equipped with Pan-Tilt-Zoom functionality can be controlled directly within the SCC client software. These controls can be found within live views whenever the cursor comes closer to the image panel, the onscreen PTZ control will appear.



Pan and Tilt

The pan and tilt functionalities can be controlled with the directional pad.

Clicking the right or left arrow will pan the camera by one step in the direction clicked. Clicking the up or down arrow will tilt the camera by one step in the direction clicked. Clicking diagonal arrows will combine the pan and tilt action of the adjacent arrows.

Zoom

The zoom on a camera can be controlled with the + and – buttons located inside the direction pad. Pressing the + button will increase zoom distance by 1 step. Pressing the - button will decrease zoom distance by one step.

3.4. Full Screen View

3.4.1. Entering Full Screen View

From any view, you can switch to full screen mode by clicking on the full screen button located above the main viewing window. Optionally you may also choose to view a single frame in full screen mode by double clicking on the frame.

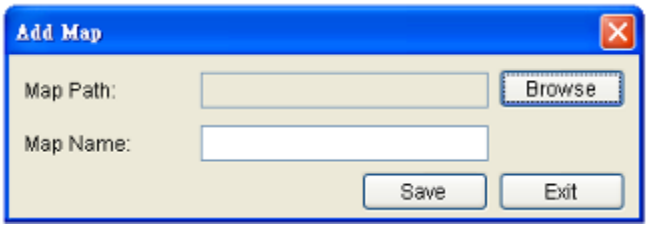
3.4.2. Exiting Full Screen Mode

To exit full screen mode, hit the **ESC** key on your keyboard.

3.5. E-Maps

3.5.1. Adding E-Maps

1. Prepare layout drawings or a map of the area being surveyed.
2. Right click on **E-Map Configuration** in the *E-map Explorer* window, Click **Add** under the *E-map* tab.



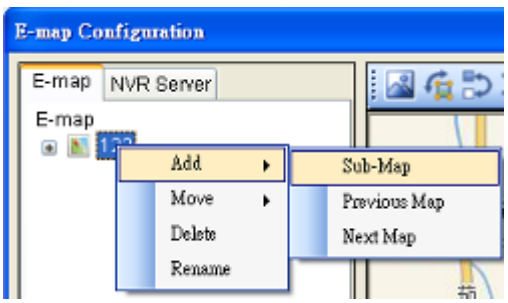
3. Click the **Browse** button to open a windows dialog. Select your map and click the **Open** button. The drawing will be stored in the Server.
4. Enter a name for the map in the **Map Name** field.
5. Click **Save**. Once successfully added, an E-map node will appear.

Note: The E-Maps can also be edited by clicking ***Server > General Tasks > E-map*** *or* ***Server Entry > Common Tasks > Common Server Tasks > E-map*** in the SCC Console.

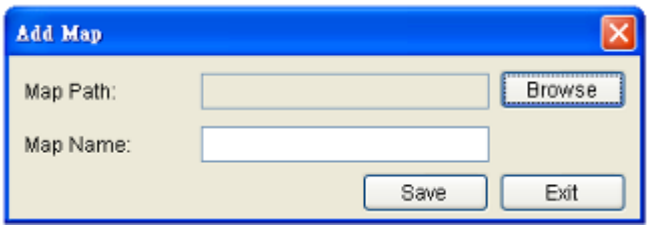
3.5.2. Adding Sub-Maps

Sub-maps can be used when separate areas within a large maps are complicated enough to have their own specific layout.

1. Prepare layout drawings or a map of the area being surveyed.
2. In the **E-map configuration** screen, under the *E-map* tab, right-click the node that you wish to add a sub-map to**,** and select **Add > Sub-Map**.



3. Click the **Browse** button to open a windows dialog. Select your map and click the **Open** button. The drawing will be stored in the Server.

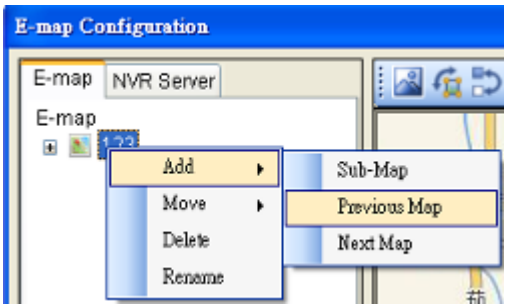


4. Enter a name for the map in the **Map Name** field.
5. Click **Save**. Once successfully added, an E-map node will appear as a sub-node on the tree panel. A link with the sub-map name will also be placed on the root map.

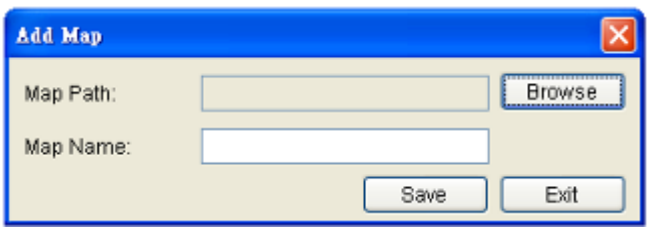
3.5.3. Adding Additional E-Maps

The typical E-map **Add** function will add new maps to the end of the list. You may choose to add a map before or after an existing map by:

1. Prepare layout drawings or a map of the area being surveyed.
2. In the E-map configuration screen, under the *E-map* tab, right-click the node which you want to add a map before or after. Choose **Add > Previous Map** to add a map before the selected map, or choose **Add > Next Map** to add a map after the selected map.



3. Click the **Browse** button to open a windows dialog. Select your map and click the **Open** button. The drawing will be stored in the Server.



4. Enter a name for the map in the **Map Name** field.
5. Click **Save**. Once successfully added, an E-map node will appear as in the tree panel.

In the e-maps list, it is recommended to organize your e-maps in a logical order.

3.5.4. Changing E-Map Order

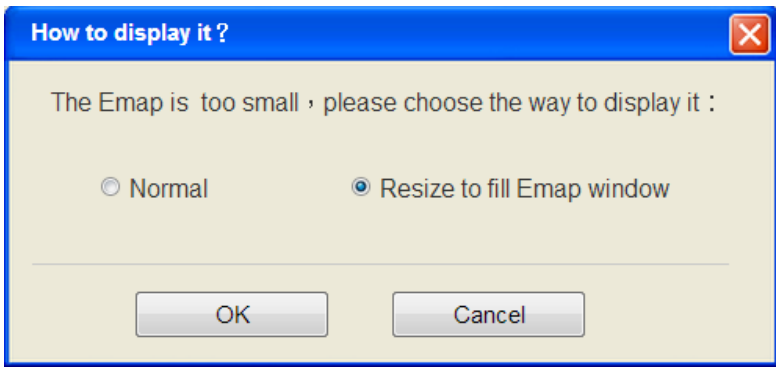
To re-order the e-maps you have added, right-click the node which you want to move. Choose **Move > Previous Map** to move the selected map up the list, or choose **Move > Next Map** to move the selected map down the list.

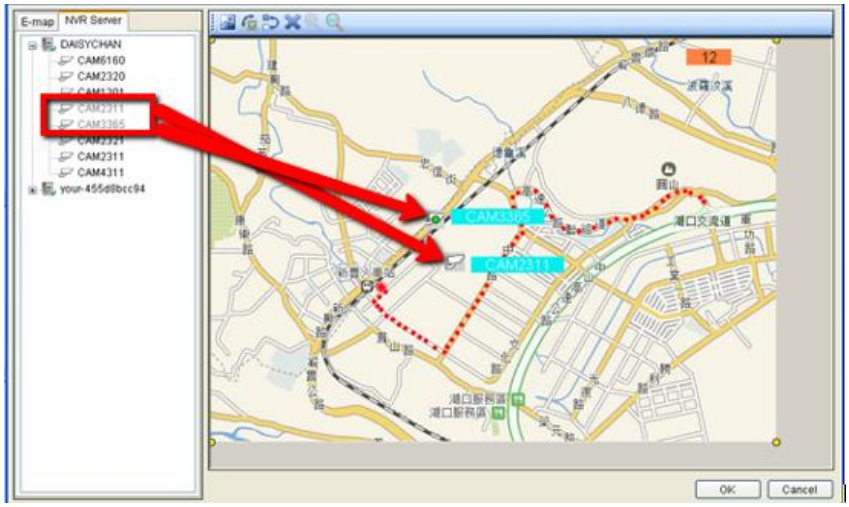
3.5.5. Renaming an E-Map

To rename an e-map you have added, right-click the node which you want to delete and choose **Rename**. Enter a new name for the map and press enter to save your changes.

3.5.6. Configuring an E-Map

1. Select an E-map entry clicking it.
2. Click the *NVR Server* tab to bring up a list of the cameras available for placement.
3. Drag and drop cameras to anywhere on the layout drawing. The map may be moved by clicking and dragging the map, you may also zoom in and out using the buttons above the map display. If the map size is lower than 396x247, you'll be prompted to select Normal or Resize to fill Emap window. The default setting is Resize to fill Emap window.





4. Once a camera icon is placed, it may be rotated by clicking one of the dotted corners of the camera icon.

5. You may save any time by clicking on the **Save** button located above the map display.

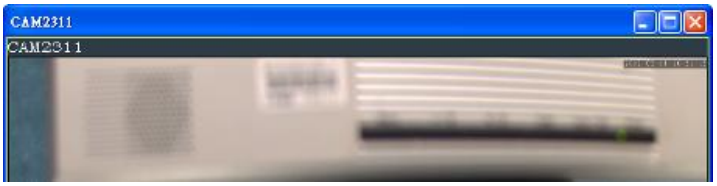
3.5.7. Deleting an E-Map

To delete an e-map you have added, right-click the node which you want to delete and choose **Delete**. This action will delete the node and any sub-nodes from the map list.

3.5.8. Using the E-Map

Once E-Maps have been configured on the system, you can pull up an E-Map by double clicking its entry in the *E-Maps* section of the Live View screen. This will open the E-Map in a floating window.

Double-clicking on any camera icon that has been placed on the map will bring a live view screen for this camera.



You can choose to do instant playback, snapshot capture and alarm management by right clicking on the live view screen.

The camera icons that have been placed on the map will blink if there is an alarm associated with it. Double-click on any camera icon to bring up a live video feed in a popup window.

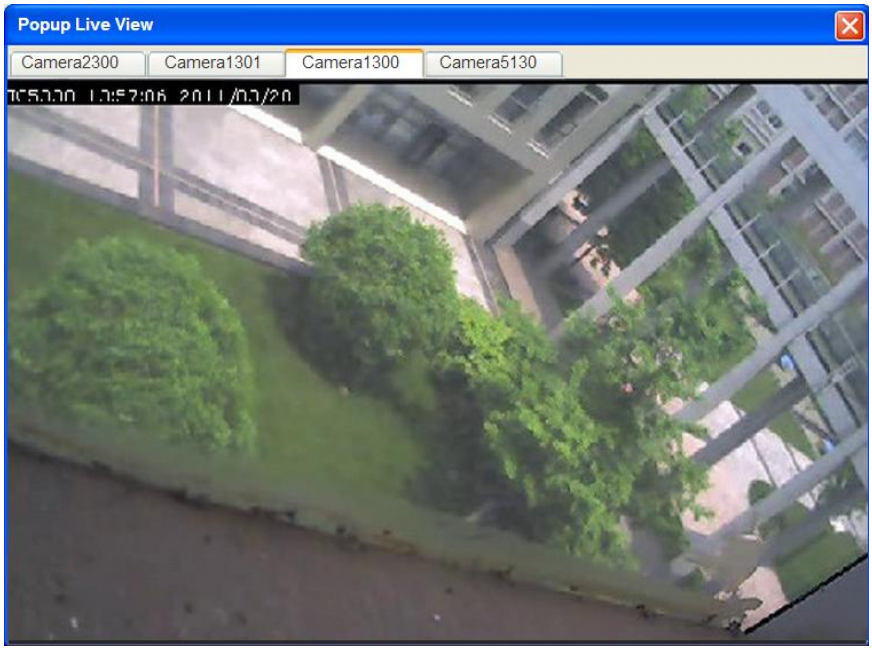
There are also a few buttons associated with this view:

Zoom Out: Located at the bottom mid-left. This button shrinks the background map display.

Zoom In: Located at the bottom mid-right. This button enlarges the background map display.

Arrows: Located on the top left. Use the arrow keys to move from map levels.

Up to 4 cameras can be popped up at the same time, when there's any alarm triggered. If there's a fifth alarm occurs, the SCC will close the oldest popup window and show the new popup.



Chapter 4. Server Setup

This section deals with Server setup procedures.

4.1. Server Basic Functions

When you are logged into a domain, the Servers configured on the domain will appear in the *Device Browser* area. The icon by the Server shows the current connection state of the Server.

Icon	Meaning
	The Server cannot be reached
	The Server can be reached, but the user is not logged in
	The user is logged in to the Server

4.1.1. Logging into a Server

1. Right-click the server entry in the *Device Browser* window to bring up the options popup.
2. Highlight and click the **Login** option. As long as the credentials supplied at the beginning of the session are correct, you will be automatically logged in.

4.1.2. Logging out of a Server

1. Right-click the server entry in the *Device Browser* window to bring up the options popup.
2. Highlight and click the **Logout** option to bring up the logout dialog box.
3. Press the **Yes** button to logout.

Note: Logging out of the domain server will cause the client to logout completely.

4.1.3. Renaming a Server

You must be connected to a server as an admin to rename it. To rename a Server:

1. Right-click the server entry in the *Device Browser* window to bring up the options popup.
2. Highlight and click the **Configuration > Rename** option.
3. Type the new name in the box that appears.

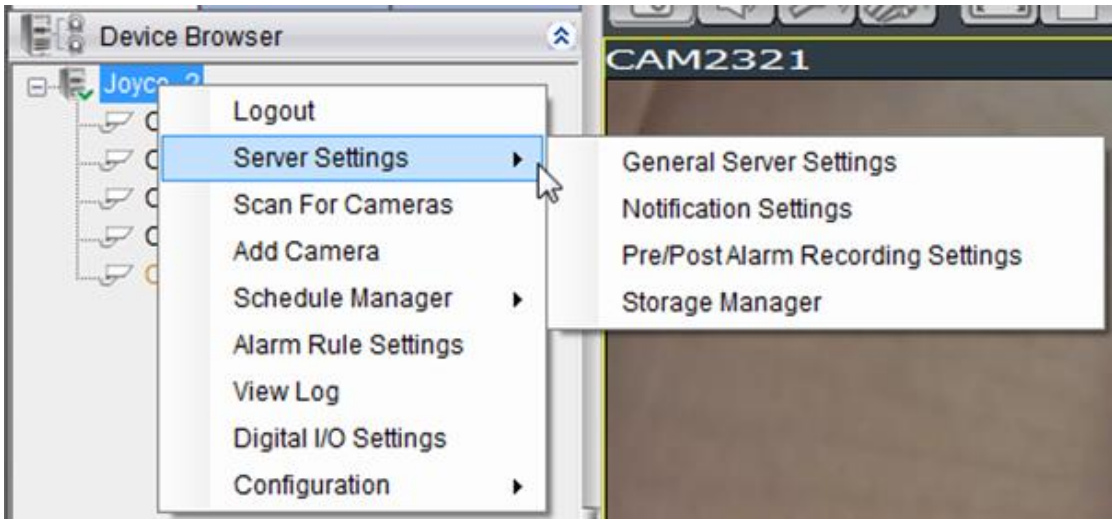
4.1.4. Viewing Server and Client Information

1. Right-click the server entry in the *Device Browser* window to bring up the options popup.
2. Highlight and click the **Configuration > About** option to bring up the *About* dialog box.
3. Click **OK** when finished viewing.

Note: The Server and Client information can also be viewed by clicking ***Others > Other Tasks > About*** in the SCC Console.

4.2. Server Settings

The following sections deal with Server settings that can be configured under the *Server Settings* menu.

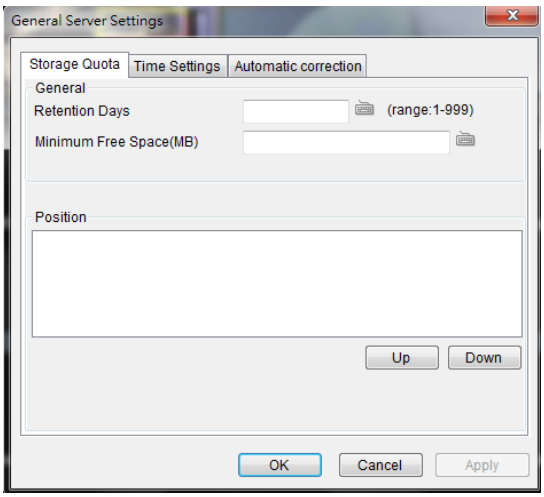


4.2.1. General Server Settings

Server general setup procedures involve configuring both storage and server time settings. To perform Server general setup:

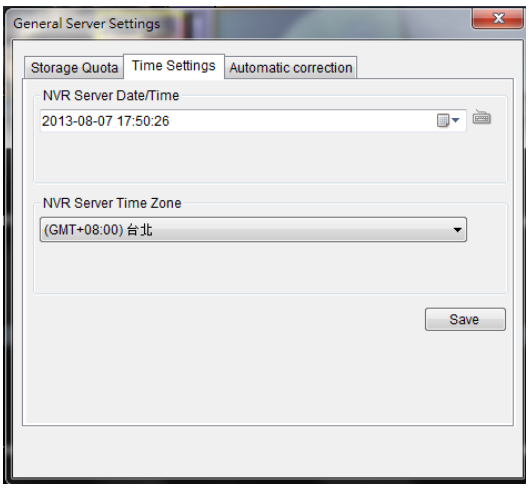
Right-click the Server entry in the *Device Browser*, highlight and click the **Server Settings > General Server Settings** option. A tabbed window will appear providing the following configuration tabs: *Storage Quota, Time Settings, and Automatic Correction*.

1. **Storage Quota**



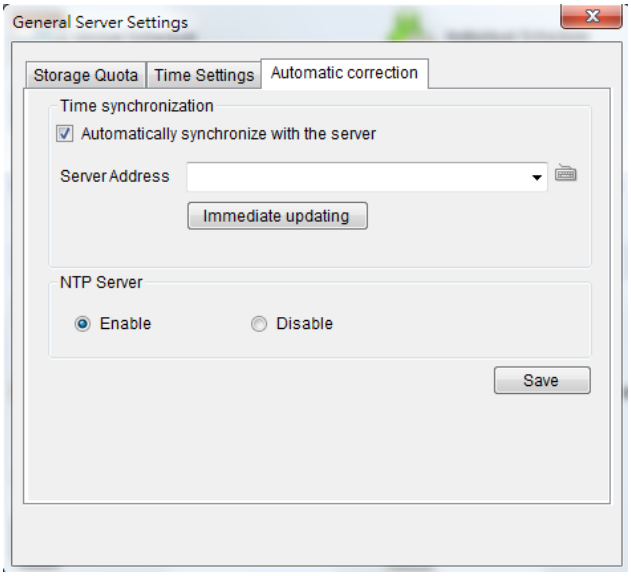
In the **Minimum Free Space** field, the Minimum space required for storage is shown. The storage will be last for 3 days. You may move the saving locations up and down the list using the **Up** and **Down** buttons, to change the storage priorities.

2. Time Settings



To set the server time click on the number you wish to change and enter a value. Click **OK** to preserve the setting. The default time is set according to the real-time clock on server.

3. Automatic Correction



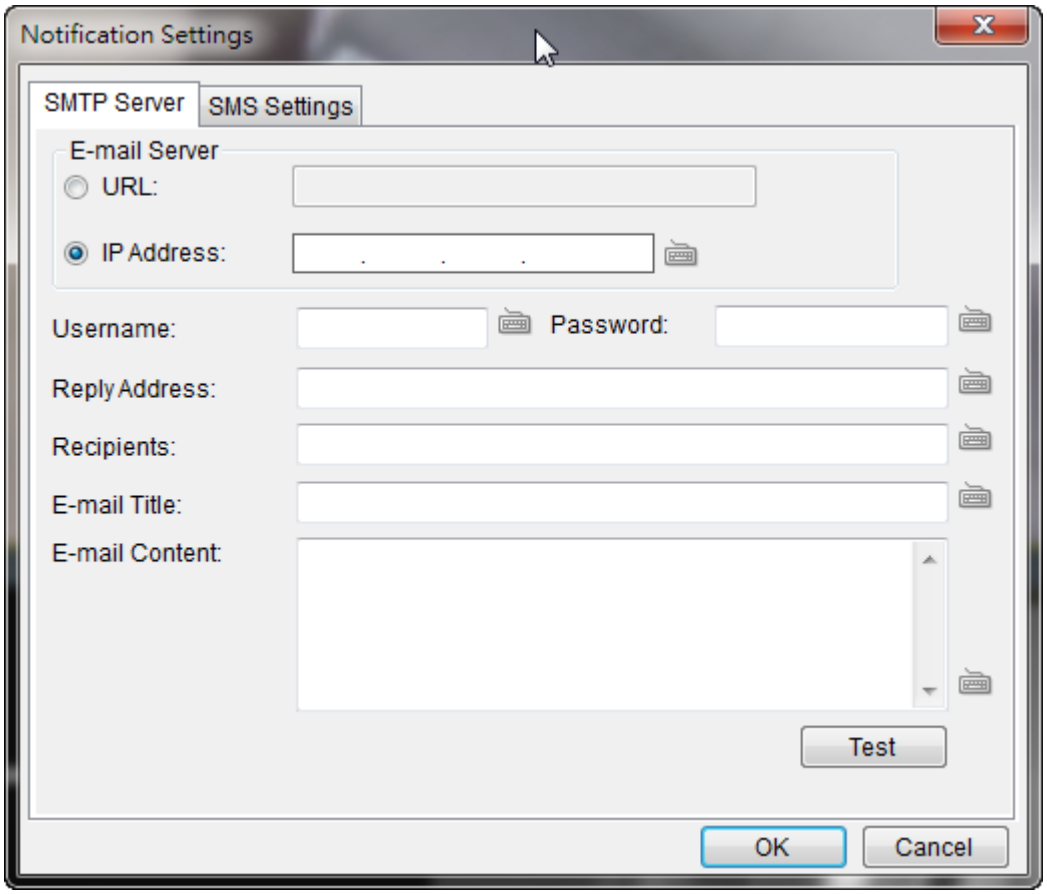
Time can be synchronized with a chosen server, typing the desired server IP address in the blank.

Select “Enable” to set your SMR/NVR device as your NTP Server and the camera time can be synchronized with your SMR/NVR device. Click **OK** to finish the configuration.

Note: General Server Settings can also be configured by clicking ***Server*** > ***General Tasks*** > ***General Server Settings*** in the SCC Console.

4.2.2. To perform Notification Setting

1. Right-click the Server entry in the *Device Browser* highlight and click the **Server Settings> Notification Setting** option. A tabbed window will appear prompt providing the following configuration tabs: *SMTP Server* and *SMS Settings*. The window starts with the *SMTP Server* tab displayed.



2. In the *SMTP Server* tab, under the *E-mail Server* heading, you may either enter the URL (such as smtp.abc.com) or IP address of the SMTP server that the Server will use to deliver E-mail notifications. The SMTP server configured here must support Unicode Transformation Format-8 (UTF-8) encoding.

3. Enter the user name for the Server email account in the **Username** field.

4. Enter the password for the Server email account in the **Password** field.

5. Enter a valid E-mail address in the **Reply Address** field. This address will be the default sender listed in E-mails sent from the Server.

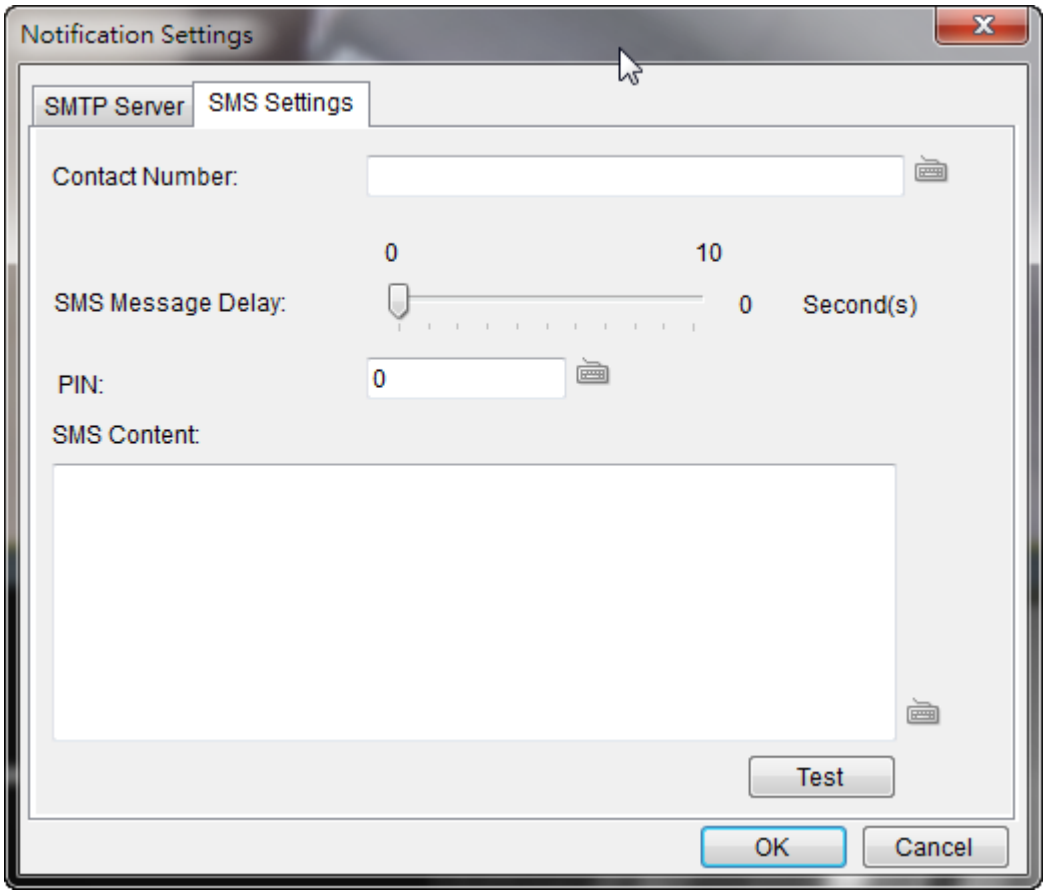
6. Enter one or more E-mail addresses in the **Recipients**: field. These address(es) will receive notifications from the Server. Multiple addresses can be entered by separating individual addresses with semi -colons ";".

7. Enter the subject of your notification E-mails, e.g., Server-xxxsite1notification in the **E- Mail Title** field.

8. Enter a short message in the large field to describe the Server or a surveillance network.

9. **(Optional)** Click **Test** to send a test message to the E-mail addresses listed.

10. Click the *SMS Settings* tab to continue.



Note: Drivers for supported GSM/GPRS modems have already been installed on the server. Currently, only the **WaveCOM-M1206B** is supported. Use COM1 on the Server to connect to a GSM modem.

11. In the **Contact Number** field, enter the phone numbers that will receive SMS notifications. Be sure to include the area code, e.g., "86",

in front of phone numbers. Use commas, "," to separate individual phone numbers.

12. Use the slider bar to select a delay between the occurrence of an event and SMS message delivery.

13. **(Optional)** If a SIM PIN is required, enter the PIN code in the **PIN** field. Note that applying incorrect PIN code may disable your SIM card.

Note: To change the PIN code, remove the SIM card from your GSM modem. Use a cell phone to change the PIN code and then re -install SIM card into the GSM modem. Changing PIN codes is not recommended because a configuration failure may disable your SIM card.

14. In the **SMS Content** field, type a simple description to include in the outgoing SMS messages

15. **(Optional)** Click **Test** to send a test message to the phone numbers listed.

16. Click the **Apply** button to apply the changes.

17. Click the **OK** button to exit E-mail/SMS settings.

Note: E-mail and SMS Settings can also be done by clicking ***Server*** > ***General Tasks*** > ***E-mail/SMS*** in the SCC Console.

4.2.3. Pre/Post Alarm Recording Settings

Video streams are constantly processed and cached in memory. The Server can trace back and preserve video/images from several minutes before and after the occurrence of an alarm.

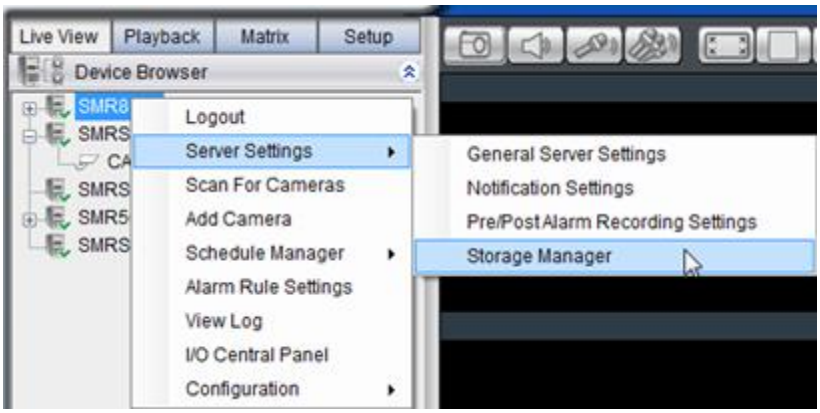
To configure pre/post-alarm recording times, highlight and click the **Pre/Post Alarm Recording Settings** option under **Server Settings**. The following pop-up window will appear:

In each of the boxes enter values for the Pre and Post-Alarm Recording times from 5 to 45 minutes (default is 45 minutes). Click the **OK** button to finish the process.

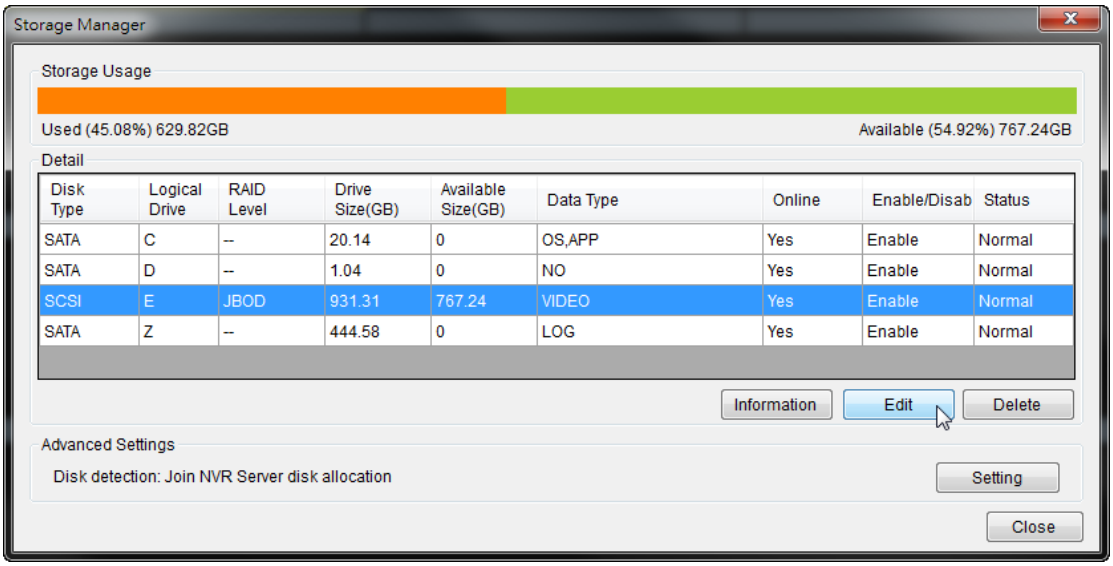
> **Note:** Pre/Post Alarm Recording Settings can also be done by clicking ***Server*** > ***General Tasks*** > ***Pre/Post Alarm Recording Settings*** in the SCC Console.

4.2.4. Storage Management

1. To access the information about the drives configured in your Server, highlight and click the **Storage Manager** option under **Server Settings**.

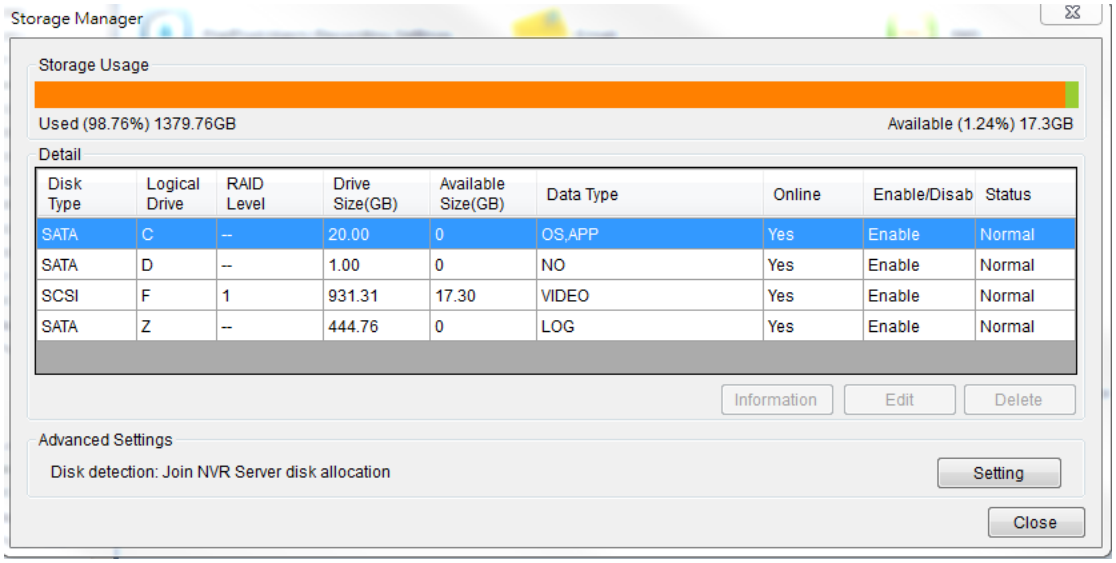


2. All available Logical Drives, as well as their sizes, free space, and status will appear. Click **Edit** to set the log and location for saving the video recordings.

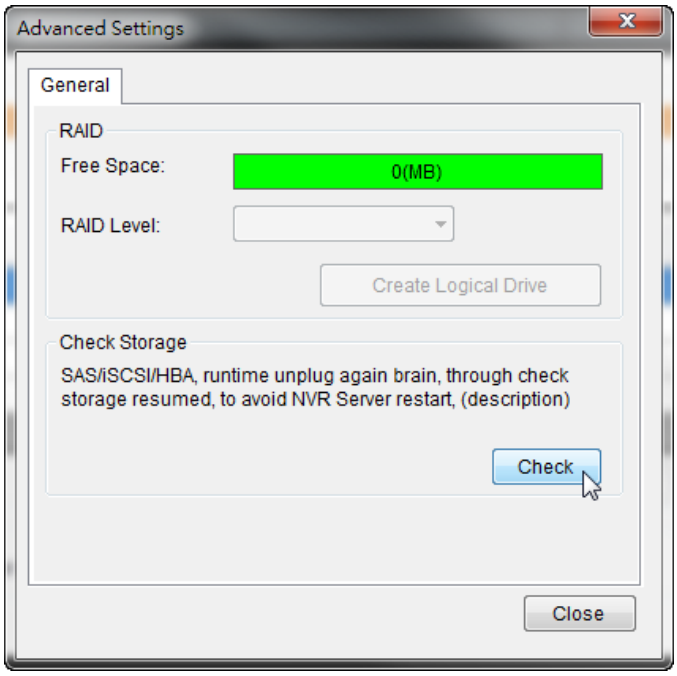

Storage Manager
Storage Usage
Used (45.08%) 629.82GB
Available (54.92%) 767.24GB
Detail
Disk Type | Logical Drive | RAID Level | Drive Size(GB) | Available Size(GB) | Data Type | Online | Enable/Disab | Status
SATA | C | -- | 20.14 | 0 | OS,APP | Yes | Enable | Normal
SATA | D | -- | 1.04 | 0 | NO | Yes | Enable | Normal
SCSI | E | JBOD | 931.31 | 767.24 | VIDEO | Yes | Enable | Normal
SATA | Z | -- | 444.58 | 0 | LOG | Yes | Enable | Normal
Information
Edit
Delete
Advanced Settings
Disk detection: Join NVR Server disk allocation
Setting
Close

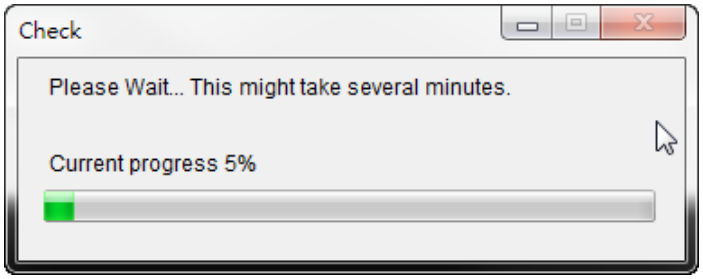
(Step 3 and 4 are for the remote client of NVR2000/SMR Series.)

3. Click the target drive first and then **Settings.**


Storage Manager
Storage Usage
Used (98.76%) 1379.76GB
Available (1.24%) 17.3GB
Detail
Disk Type | Logical Drive | RAID Level | Drive Size(GB) | Available Size(GB) | Data Type | Online | Enable/Disab | Status
SATA | C | -- | 20.00 | 0 | OS,APP | Yes | Enable | Normal
SATA | D | -- | 1.00 | 0 | NO | Yes | Enable | Normal
SCSI | F | 1 | 931.31 | 17.30 | VIDEO | Yes | Enable | Normal
SATA | Z | -- | 444.76 | 0 | LOG | Yes | Enable | Normal
Information
Edit
Delete
Advanced Settings
Disk detection: Join NVR Server disk allocation
Setting
Close

In “Advanced Settings” dialogue, “General” tab, click **Check**.





4. Choose the RAID level, and then click Create Logical Drive to create the RAID configuration.

Note: Storage Manager can also be accessed by clicking ***Server > General Tasks > Storage*** *or* ***Server Entry > Common Tasks > Common Server Tasks > Storage*** in the SCC Console.

4.3. Scheduling Recording

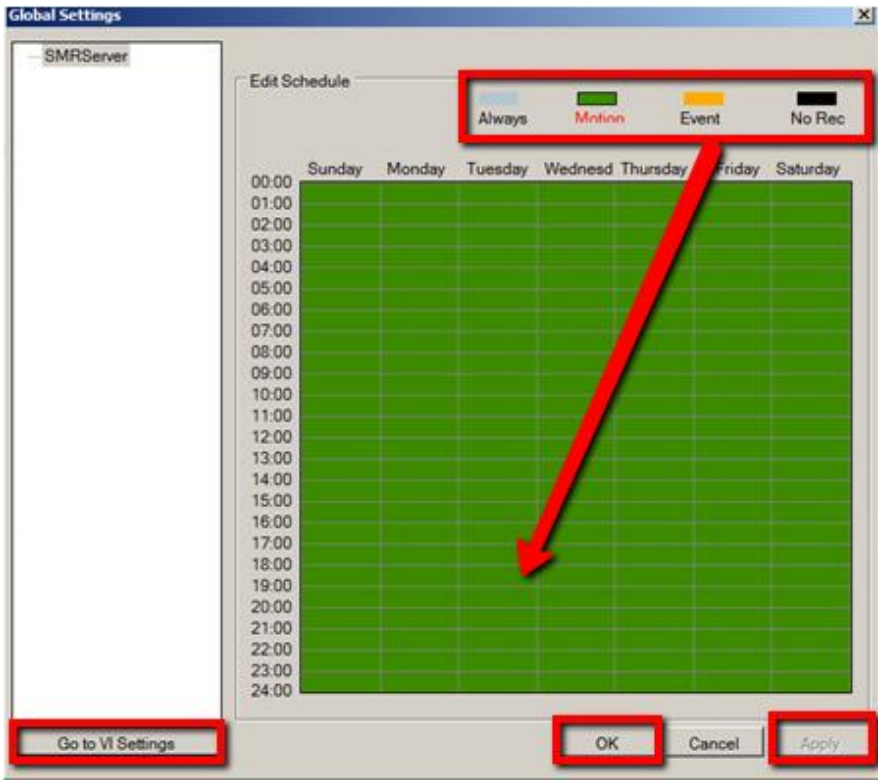
There are two forms of scheduling available. A global schedule can be created to apply to an entire Server, while an individual schedule can be created for each camera on a Server. Schedules are further split into weekly and daily schedules. When scheduling conflicts occur, the daily schedule takes precedence over the weekly schedule.

4.3.1. Global Scheduling

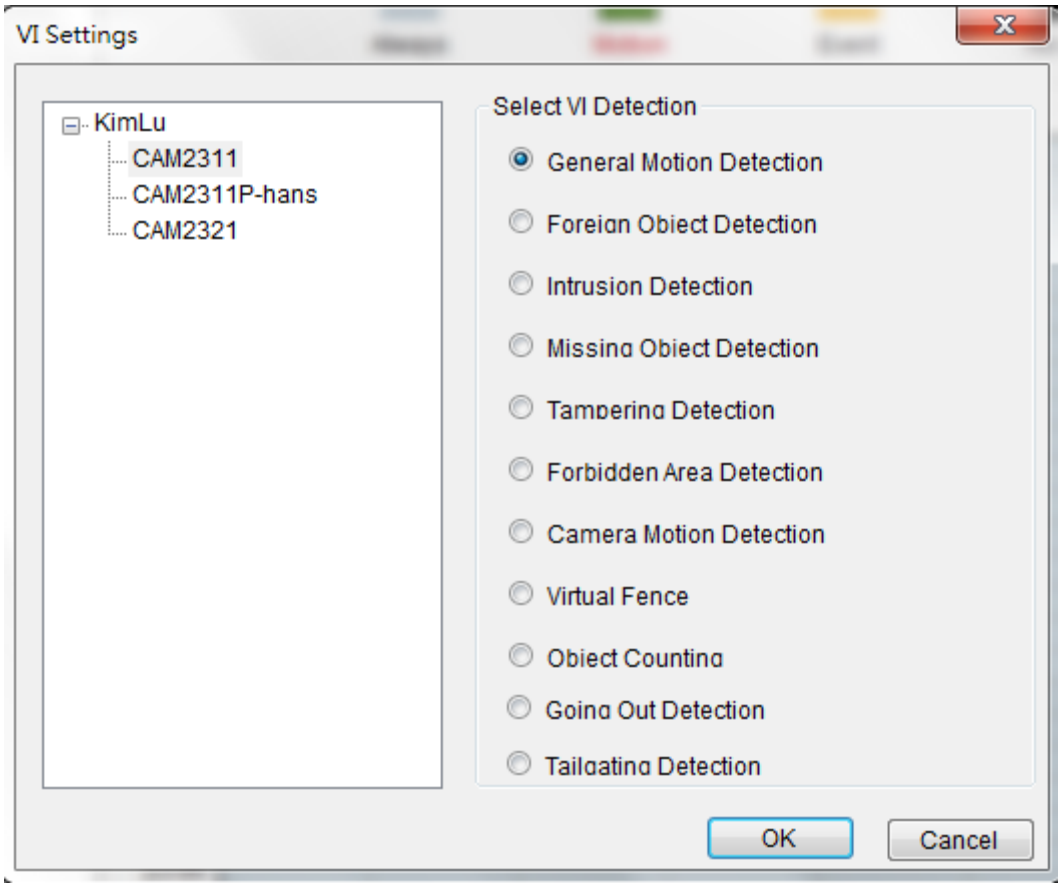
Note: A global schedule can also be set by clicking ***Server*** > ***General Tasks*** > ***Global Schedule*** *or* ***Server Entry*** > ***Common Tasks*** > ***Common Server Tasks*** > ***Storage*** in the SCC Console.

Weekly Global Scheduling

To access the Global Scheduling tool right click the Server entry, then highlight and click the **Schedule Manager** > **Global Settings** option to bring up a popup containing a schedule grid corresponding to every hour of every day in the week. The schedule default is always recording, all the time. To change the global schedule:



1. Choose a recording method by clicking on one of the four methods: **Always** record or record on **Event** trigger. (You can also keep the default as **Motion** record.)
2. Click on a table cell to "paint" the recording method. The color in the cell will change to match the selected recording method. Click and drag the cursor to paint large areas.
3. When you are finished, click the **Apply** button to apply the schedule.
4. **(Optional)** You may go to the VI setting panel by clicking **Go to VI Settings.**



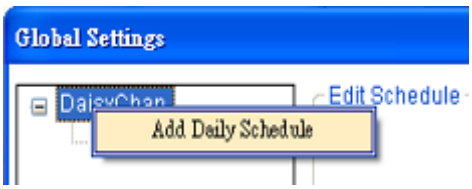
5. Click **OK** to exit the menu.

Daily Global Scheduling

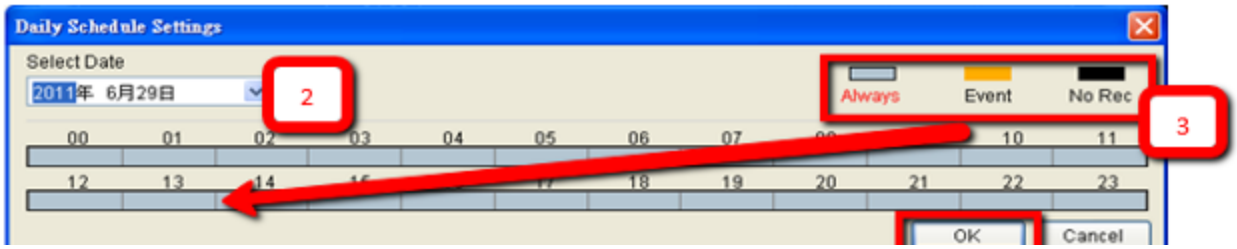
Adding a Daily Global Schedule

In addition to the weekly global schedule, a daily schedule can also be set for a certain day. To perform this action:

1. Under *Global Settings*, right-click the server listing, and click on the **Add Daily Schedule** option to bring up the *Global Daily Schedule Settings* popup. This popup consists of 24 segments corresponding to the hours in the day.



2. Choose the date that you want to schedule.



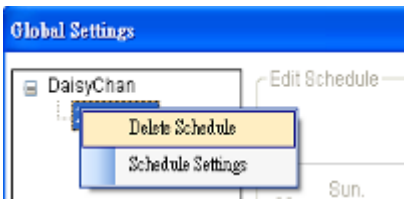
3. Choose a recording method by clicking on one of the three methods: **Always** record, record on **Motion** detection, or record on **Event** trigger.

4. Click on a table cell to "paint" the recording method. The color in the cell will change to match the selected recording method. Click and drag the cursor to paint large areas.

5. When you are finished, click the **OK** button to apply the schedule. The schedule will show up under the server entry in the *Global Settings* according to the date you have just set.

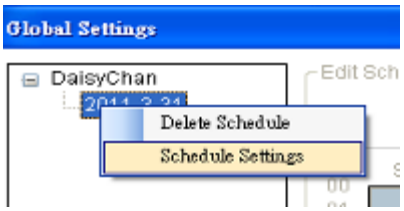
Deleting a Global Daily Schedule

To delete a global daily schedule, right-click the schedule entry and select **Delete Schedule.** Click the **Yes** button to confirm deletion.



Editing a Global Daily Schedule

To edit a global daily schedule, right-click the schedule entry and select **Schedule Settings**.



4.3.2. Individual Scheduling

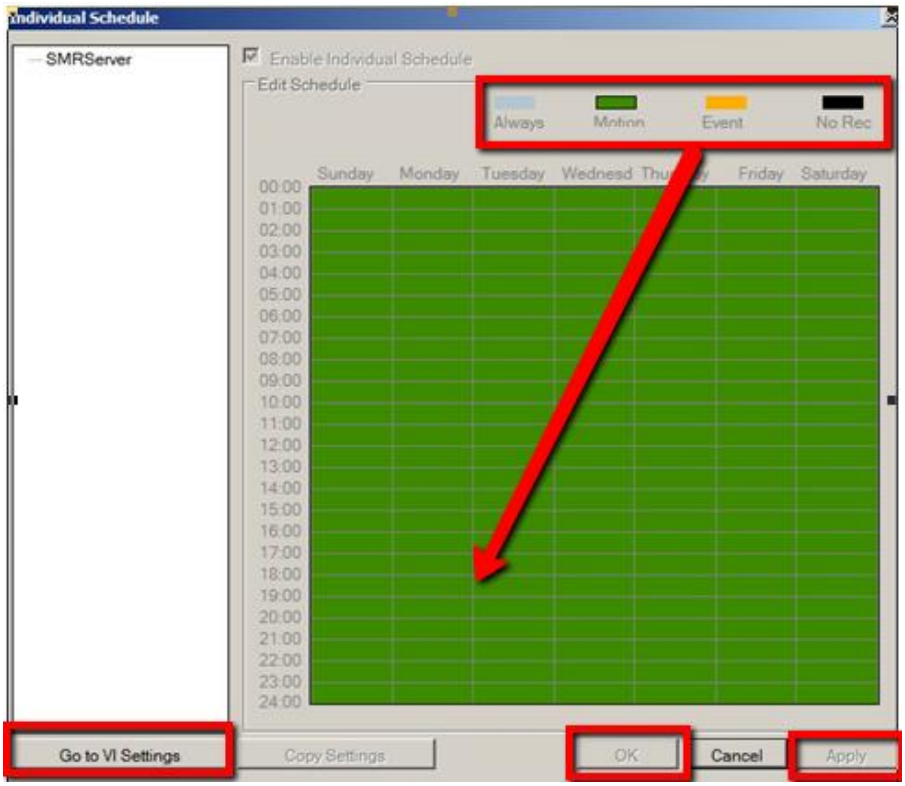
Individual schedules, which take precedence over the global schedule, can be set for each camera.

Note: An individual schedule can also be set by clicking ***Server > General Tasks > Individual Schedule*** in the SCC Console.

Weekly Individual Scheduling

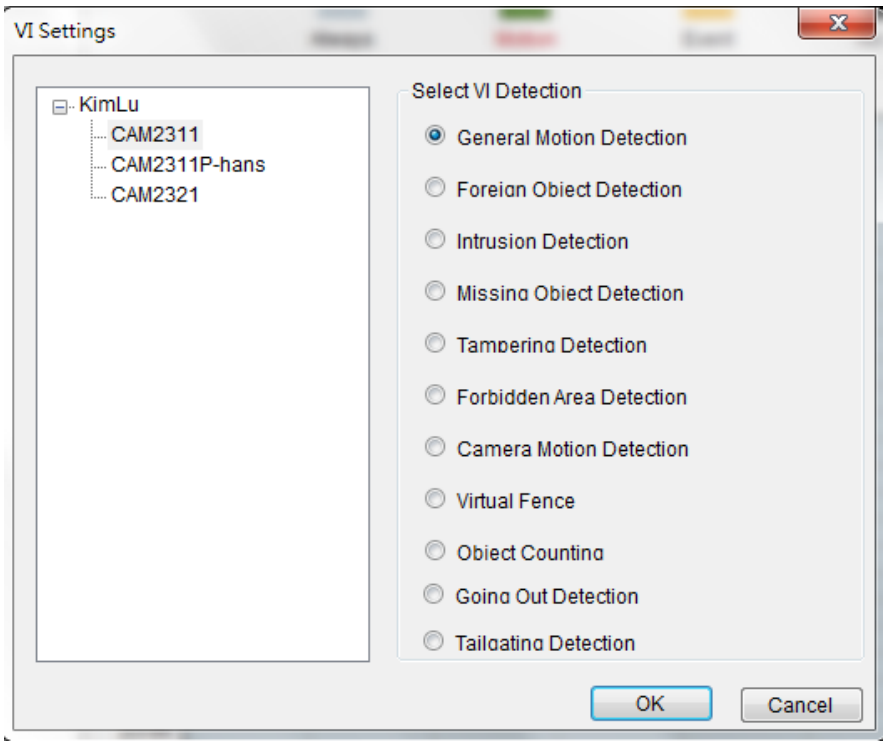
To access the individual scheduling tool right-click the server entry, then highlight and click **Schedule Manager > Individual Schedule.**

Schedule defaults are always recording, all the time. To create a schedule:



1. Select the camera which you want schedule.
2. Click the **Enable Individual Schedule** box to enable the schedule.
3. Choose a recording method by clicking on one of the four methods:

   Always record or record on **Event** trigger. (You can also keep the default as **Motion** record.)
4. Click on a table cell to "paint" the recording method. The color in the cell will change to match the selected recording method. Click and drag the cursor to paint large areas.
5. When you are finished, click the **Apply** button to apply the schedule.
6. **(Optional)** You may go to the VI setting panel by clicking **Go to VI Settings.**



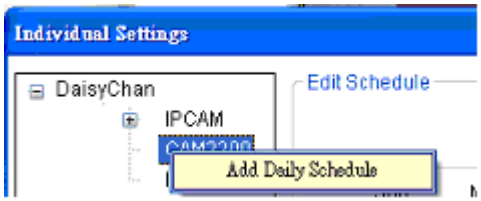
7. Click **OK** to exit the menu.

Daily Individual Scheduling

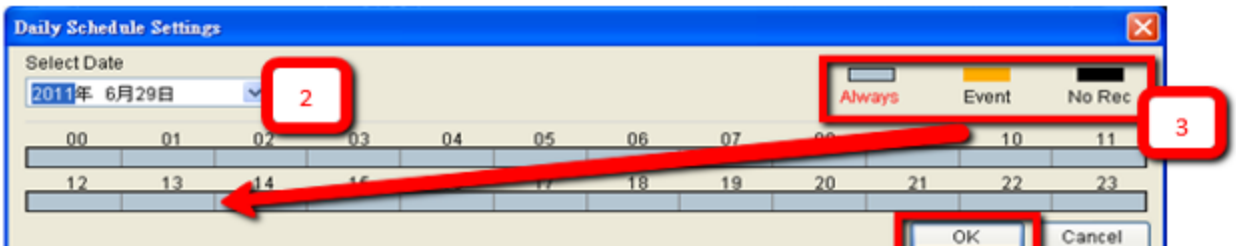
Adding a Daily Individual Schedule

In addition to the weekly individual schedule, a daily schedule can also be set for a certain day. To perform this action:

1. In *Weekly Individual Schedule* right-click the camera listing, and select **Add Daily Schedule** option to bring up the *Individual Daily Schedule Settings* popup. This popup consists of 24 segments corresponding to the hours in the day.



2. Choose the date that you want to schedule



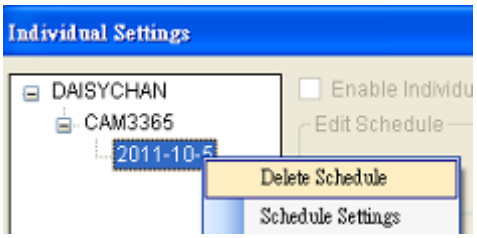
3. Choose a recording method by clicking on one of the three methods: **Always** record, record on **Motion** detection, or record on **Event** trigger.

4. Click on a table cell to "paint" the recording method. The color in the cell will change to match the selected recording method. Click and drag the cursor to paint large areas.

5. When you are finished, click the **OK** button to apply the schedule. The schedule will show up under the camera entry in the *Individual Settings* according to the date you have just set.

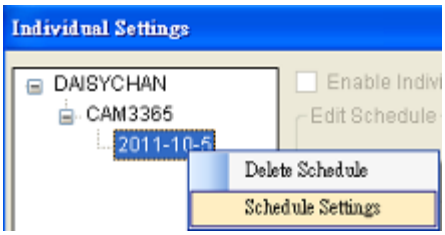
Deleting an Individual Daily Schedule

To delete an individual daily schedule, right-click the schedule entry and select **Delete Daily Schedule.** Click **Yes** to confirm deletion.



Editing an Individual Daily Schedule

To edit an individual daily schedule, right-click the schedule entry and select **Schedule Settings.**



Chapter 5. Camera Setup

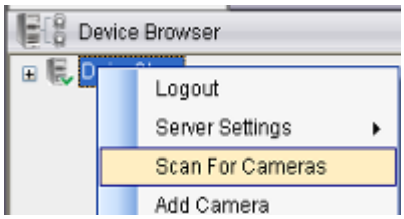
This section deals with Camera setup procedures. These options can be accessed by right-clicking the Camera entry in the *Device Browser*.

5.1. Adding Cameras

Cameras can be added to the Server in two ways, VIA and automatic scan, or by manually inputting the camera information.

5.1.1. Automatic Scan for Cameras

To begin an automatic scan for cameras:

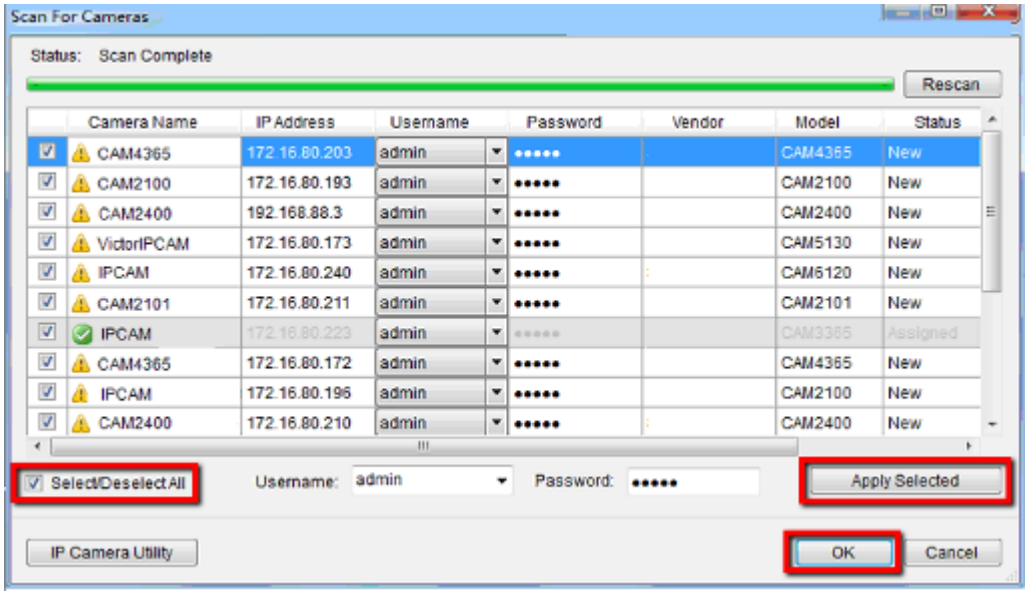


1. Right-click the Server entry and select **Scan for Cameras**. The system will respond by beginning an automatic scan. Once the scan is complete, the cameras that can be added to the Server will be displayed. Information available for each camera will include:

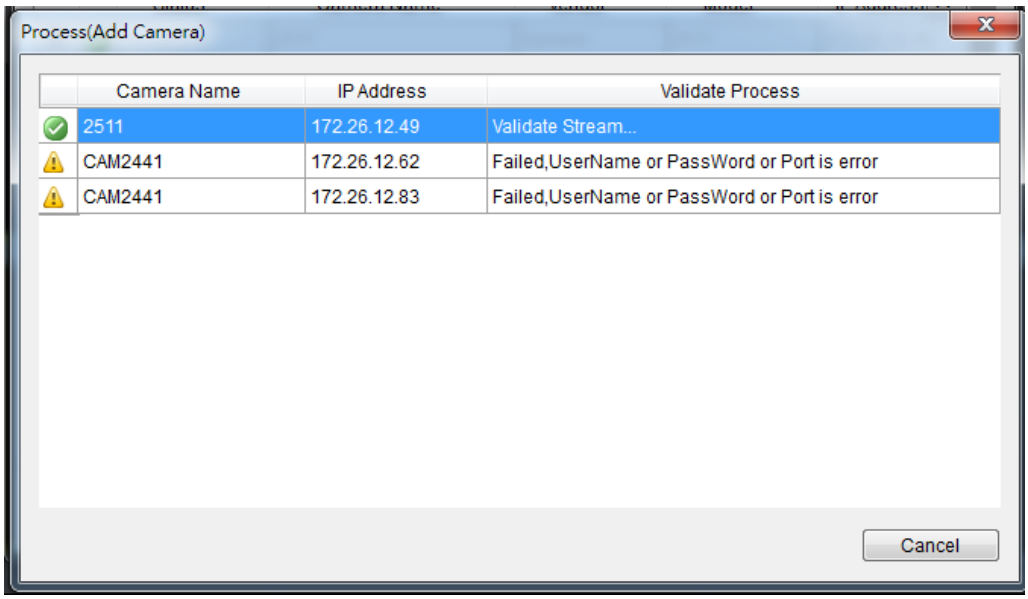
- **Name** – The default camera name (Make/Model)
- **Status** – The camera will display *New* if it has not been added to this Server, otherwise it will display *Assigned*.
- **IP Address**
- **MAC Address**
- **Vendor - Including ACTI, ASONI, AVTECH, AXIS, Arecont, Sosch, Brickcom, DyNACOLOR, D_Link, Dahua, EDIMAXHIKVISION, EverFocus, HIKVISION, IQinVision, Lilin, Eessoa, Mobotix, ONVIF, Panasonic, SIMON, SONY, Samsung, Surveon, VIVOTEK, and General.**
- **Model -** when **"General"** is selected, **"RTP over TCP"** and **"RTP over UDP"** can be further defined.

2. To add a camera to the system, check the box by the camera entry. You may also check the **Select All** box at the bottom of the window to select all the cameras found.

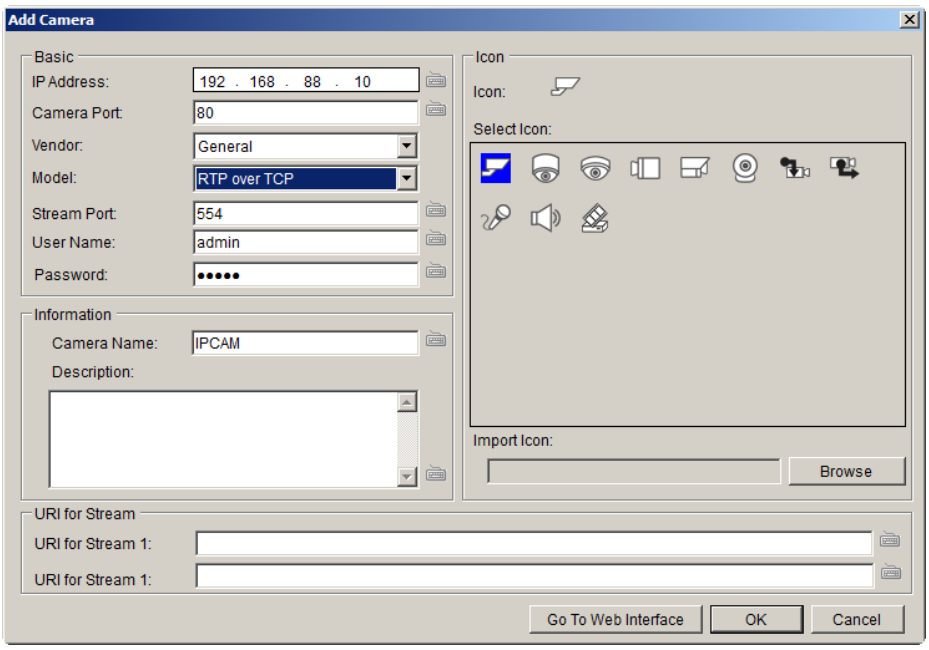
Enter the username and password, and press **Apply Selected**. Click **OK** to add the selected cameras to the Server.



The following windows will prompt for validation.



3. **(Optionally)** Double-click any camera entry to bring up the camera detail page. From this page you may change the following information:



- **IP Address** – Changing this value will affect connectivity.
- **Camera Port -** The web access port, default is 80.
- **Stream Port** – Default is 6002
- **Vendor** – Changing this value will affect connectivity.
- **Model** – Changing this value will affect connectivity.
- **User Name** – This value is not always required.
- **Password** – This value is not always required.
- **Camera Name** – It is recommended you change this value if you have more than one camera of this make/model.
- **Camera Description**
- **Camera Icon -** You can also import your own icon by clicking on the **Browse** button and choosing an icon file. Valid icon files include JPEG, GIF, PNG, BMP and ICON files.

Finally, you can access the web interface for the camera by clicking on the **Go to Web Interface** button. Click **OK** to save your changes, or **Cancel** to exit without saving.

4. **(Optionally)** You may access the IP Utility for camera configurations by clicking the **IP Camera Utility** button.

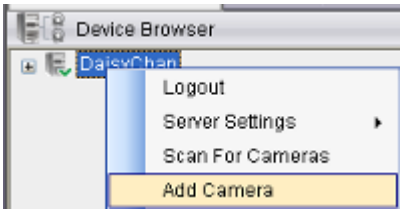
5. Click **OK** to add the selected cameras to the Server.

Note: Automatic Scan for Cameras can also be accessed by clicking ***Camera List*** > ***General Tasks*** > ***Scan for Cameras*** *or* ***Server Entry*** > ***Common Tasks*** > ***Common Server Tasks*** > ***Scan for Cameras*** in the SCC Console.

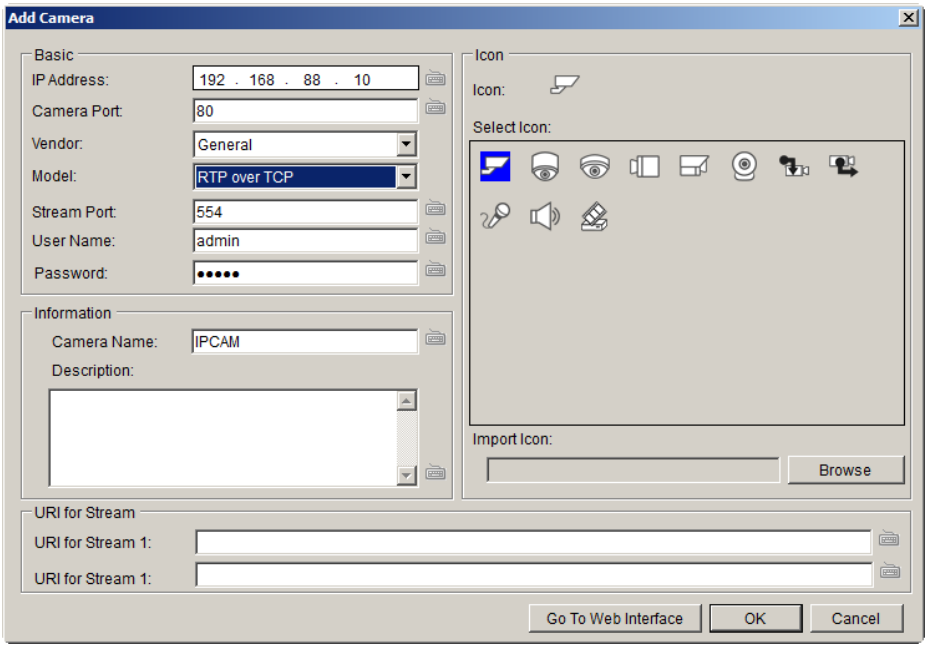
5.1.2. Manually Adding Cameras

To manually add a camera to the Server:

1. Right-click the Server entry and select **Add Camera**.



2. In the camera window fill out the following information:



- **IP Address**
- **Camera Port** - This value will automatically populate with the default value for the **Vendor** and **Model** selected.
- **Vendor - Including ACTI, ASONI, AVTECH, AXIS, Arecont, Sosch, Brickcom, DyNACOLOR, D_Link, Dahua, EDIMAXHIKVISION, EverFocus, HIKVISION, IQinVision, Lilin, Eessoa, Mobotix,**

ONVIF, Panasonic, SIMON, SONY, Samsung, Surveon, VIVOTEK, and General.

- **Model -** when **"General"** is selected, **"RTP over TCP"** and **"RTP over UDP"** can be further defined.
- **Stream Port** - This value will automatically populate with the default value for the **Vendor** and **Model** selected.
- **User Name** – This value is not always required.
- **Password** – This value is not always required.
- **Camera Name** – It is recommended you change this value if you have more than one camera of this make/model.
- **Camera Description**
- **Camera Icon -** You can also import your own icon by clicking on the **Browse** button and choosing an icon file. Valid icon files include JPEG, GIF, PNG, BMP and ICON files.

3. Finally, once basic camera information is filled in, you may access the web interface for the camera by clicking on the **Go to Web Interface** button. Click **OK** to add the camera.

Note: Cameras can also be added manually by clicking ***Camera List*** > ***General Tasks*** > ***Add Camera*** in the SCC Console.

5.1.3. Deleting a Camera

1. Right-click the camera entry you wish to remove in the *Device Browser* window to bring up the options popup.
2. Highlight and click the **Delete Camera** option. The system will respond with a warning dialog.

   Click **Yes** to delete the camera from the Server.

Note: Cameras can also be deleted by clicking ***Camera List*** > ***General Tasks*** > ***Delete Camera*** in the SCC Console.

5.1.4. Initializing a Camera

Initializing the camera resets the camera so that it will correspond to the settings on the Server. To perform this operation:

1. Right-click the camera entry in the *Device Browser* window to bring up the options popup.
2. Highlight and click the **Initialize** option. The system will respond with a warning dialog.
3. Click **Yes** to reset the camera.

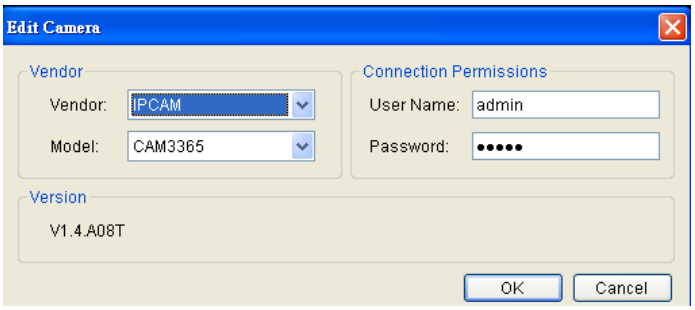
Note: Camera initialization can also be done by clicking ***Camera List*** > ***Camera Settings*** > ***Initialize*** in the SCC Console.

5.2. Camera General Settings

5.2.1. Logging into a Camera

It is important to note that you must be logged into the camera before you can change any settings. To login to the camera:

1. Right-click the camera entry and select **Camera Settings > Edit Camera**.



2. In the *Connection Permissions* section, enter a valid username in the **User Name** field and password in the **Password** field.

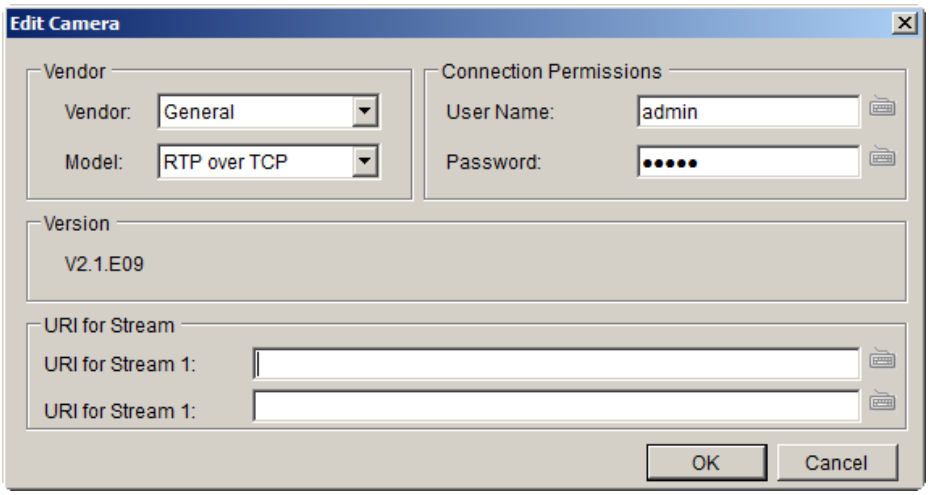
Note: The system will not perform an active check on the username and password. Setting an incorrect username or password may affect camera connectivity and configurability.

3. Click **OK** to login.

5.2.2. Changing the Camera Model and Vendor

In certain situations it may be necessary to change the Vendor or Model information for the camera. To perform this operation:

1. Right-click the camera entry and select **Camera Settings > Edit Camera**.



2. Select the new **Vendor** and **Model** from the respective drop-downs.

When there's no suitable option for your device, you can select "**General**" from the **Vendor** dropdown list and defined if it's a **"RTP over TCP"** or a **"RTP over UDP"** from the **Model** dropdown list. Once set, define URI for Stream 1.

See the reference below for further setting.

For an AXIS IP camera,
key in "RTSP://<IP of the IP camera>/<codec>/media.amp"

For a HIKVISION IP camera,
key in "RTSP://username:password@<IP of the IP Camera>"

For a Surveon IP camera,
key in "RTSP://<IP of the IP camera>/stream1 or stream2"

Note: Setting an incorrect vendor or model may affect camera connectivity.

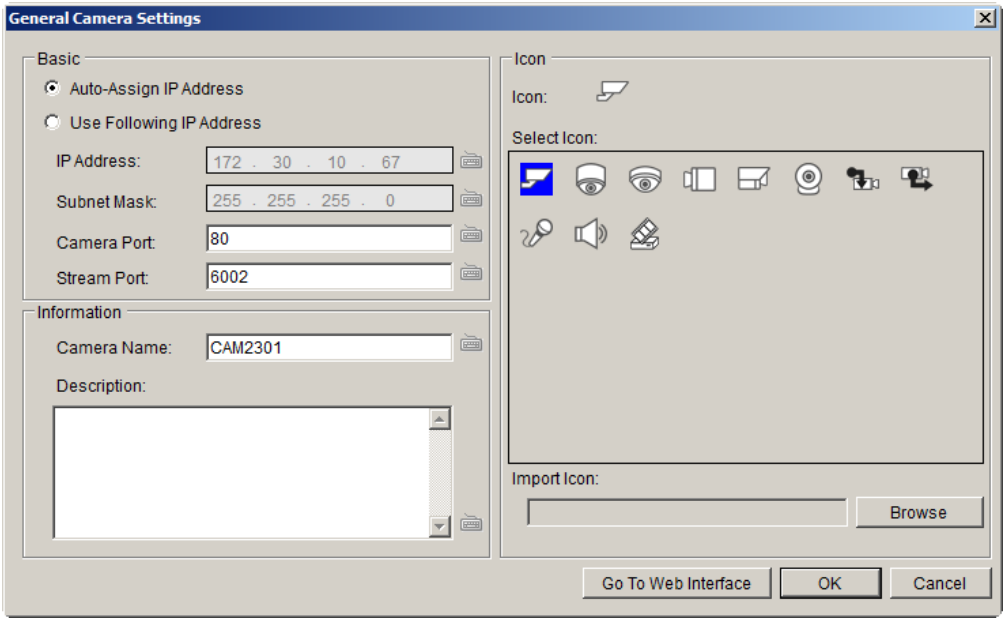
3. Click **OK** to save your changes.

Note: Edit Camera can also be accessed by clicking ***Camera List > Camera Settings > Edit Camera*** in the SCC Console.

5.2.3. General Settings

Camera general settings include network connectivity settings, as well as basic camera name, description and icon settings.

1. Right-click the camera entry and select **Camera Settings > Camera General Settings**.



2. There are two ways to specify the IP address for the camera.
   - If you wish to automatically assign an IP address to the camera using DHCP services, select the **Auto-assign IP Address** option.
   - If you wish to assign a fixed IP, select **Fixed IP Address**, and provide an IP address for the camera in the **IP Address** field. The Subnet Mask will be shown together with the IP address.
3. You may continue by editing any of the following options:
   - **Camera Port** - This value will automatically populate with the default value for the **Vendor** and **Model** selected.
   - **Stream Port** - This value will automatically populate with the default value for the **Vendor** and **Model** selected.
   - **Camera Name** – It is recommended you change this value if you have more than one camera of this make/model.
   - **Camera Description**

- **Camera Icon** - You can also import your own icon by clicking on the **Browse** button and choosing an icon file. Valid icon files include JPEG, GIF, PNG, BMP and ICON files.

4. Click **OK** to save your changes.

Note: Camera General Settings can also be configured by clicking ***Camera List*** > ***Camera Settings*** > ***Camera General Settings*** in the SCC Console.

5.2.4. OSD Settings

On cameras with OSD capabilities, these capabilities can be configured within the server. To configure the information for the on-screen display:

1. Right-click the camera entry and select **Camera Settings** > **OSD Settings** to bring up the OSD settings menu.

2. Choose any of the following options:
   - **Show Name** – Displays the camera name. If this item is selected, you will also have the option of entering another name to display.
   - **Show Date** – Displays the camera date.
   - **Show Time** – Displays the camera time.
   - **Transparent Display** – When this option is chosen, the camera will not black-out the lettering background.

3. Click **OK** to save your changes.

Note: OSD Settings can also be configured by clicking ***Camera List*** > ***Camera Settings*** > ***OSD Settings*** in the SCC Console.

5.2.5. Privacy Mask Settings

The camera can be configured to display useful information on the top bar. To configure the information for the on-screen display:

1. Right-click the camera entry and select **Camera Settings** > **Mask Settings** to bring up the privacy mask settings menu.

2. Click the **New** button to create a new privacy mask overlay, denoted by a red border.
3. Click and drag the overlay to move the overlay around the screen. Click and drag one of the six white dots on the red border to resize and reshape the overlay. If multiple windows are present, the window being edited will have a red border.
4. Repeat these steps to create up to three windows. Click **OK** to save the privacy mask.

The masked areas will be shown in black on the live view screen after the mask is saved.

Note: (1) The masked areas can be unmasked during a video export with an administrative password. For more details refer to the section on video export. (2) Privacy Mask Settings can also be configured by clicking ***Camera List > Camera Settings > Mask Settings*** in the SCC Console.

5.3. Camera Image and Quality Settings

5.3.1. Camera Image Settings

To configure camera image settings:

1. Right-click the camera entry in the *Device Browser*, then click **Image Adjustments > Image Settings**.

Note: You must be logged into the camera before changing settings or else the operation will fail.

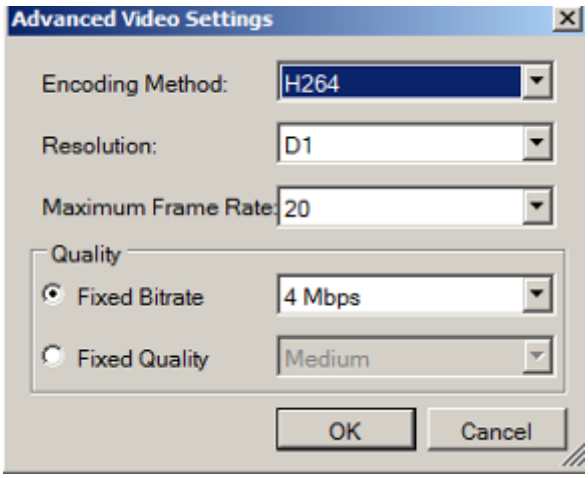
2. Adjust the following sliders to change the camera image:
   - **Brightness** – The overall lighting level of the image. This value can be used to boost or reduce the apparent lighting of the image.
   - **Saturation** – The overall color intensity of the image. This value can be used to boost or reduce overall color intensity.
   - **Contrast** – The lighting difference between dark and light areas of the image. This value can be used to boost or reduce apparent differences in lighting.
   - **Hue** – The color cast of the image. This value can be used to compensate for colored lighting or other color casting.
   - **Sharpness** – The edge contrast of the image. This value can be used to make the picture appear clearer.

3. Click **OK** to save your changes.

Note: Camera Image Settings can also be configured by clicking ***Camera List*** > ***Camera Settings*** > ***Image Settings*** in the SCC Console.

5.3.2. Advanced Video Settings

1. Right-click the camera entry in the *Device Browser*, then click **Image Adjustments > Advanced Video Settings**.



Note: You must be logged into the camera before changing settings or else the operation will fail.

2. Select a video encoding method from the **Encoding Method** drop-down. Encoding methods will vary by camera type, but common ones include:
   - **MJPEG**
   - **MPEG-4**
   - **H264**

3. Select a video resolution from the **Resolution** drop-down. Supported resolutions will vary by camera. 2M 60FPS and 3M 30FPS are supported.

   Select the maximum video frame rate from the **Maximum Frame Rate** drop-down.

4. From the *Quality* section, choose one of the following:
   - **Fixed Bitrate** – The camera image quality will be adjusted within a fixed bitrate selected in the dropdown. Dropdown values will vary by camera.
   - **Fixed Quality** – The camera bitrate will be adjusted to meet the quality selected in the dropdown. Dropdown values will vary by camera.

Note: Video Quality Settings can also be configured by clicking ***Camera List*** > ***Camera Settings*** > ***Advanced Video Settings*** in the SCC Console.

5.4. PTZ Settings

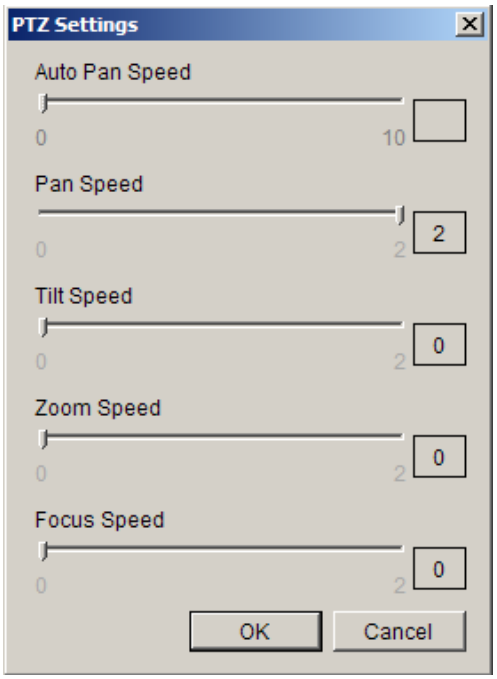
In cameras equipped with any combination of pan, tilt or zoom (PTZ) functionality, these settings are used to configure the PTZ functions.

5.4.1. PTZ Settings

The PTZ settings deal with the software PTZ control panel. These settings adjust how much the camera will pan, tilt, zoom, and focus with each control panel input.

Note: You must be logged into the camera before changing settings or else the operation will fail.

1. Right-click the camera entry in the *Device Browser*, and click **PTZ Settings > PTZ Settings**.



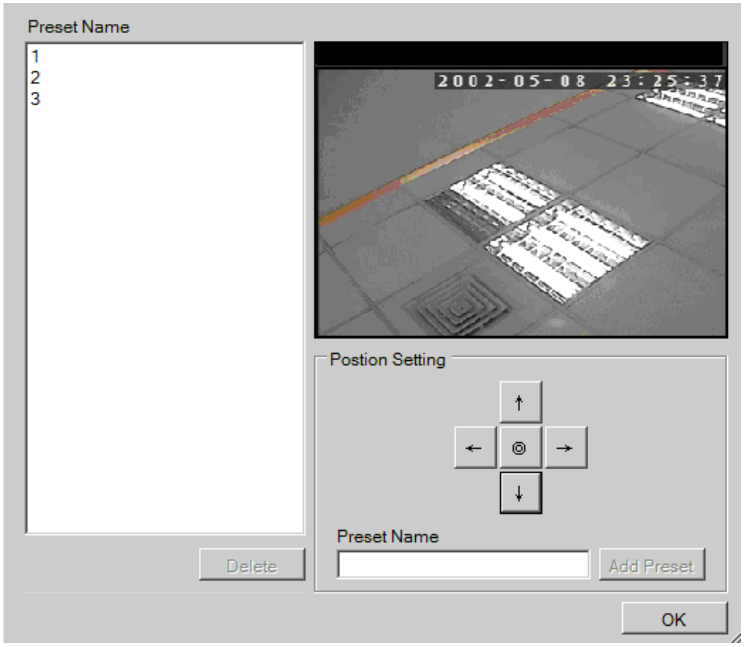
2. Adjust the following sliders to increase and decrease the following speeds: (The higher the value, the higher the speed) Unsupported features on specific cameras will be grayed out.
   - **Auto Pan Speed** – The speed which the camera will pan between the mechanical stops when the **Auto Pan** function is activated.
   - **Pan Speed** – The distance the camera will pan to each side.
   - **Tilt Speed -** The distance the camera will tilt up and down.
   - **Zoom Speed -** The distance the camera will zoom near or far.

- **Focus Speed** - The amount the camera will focus forward or backward.

Note: PTZ Settings can also be configured by clicking ***Camera List*** > ***Camera Settings*** > ***PTZ Settings*** in the SCC Console.

5.4.2. PTZ Preset Settings

Certain preset pan/tilt/zoom values can be saved in order to move the camera quickly to a point of interest. To configure camera PTZ preset settings, right-click the camera entry, then highlight and click **PTZ Settings** > **Preset Settings** option.



The popup will display the camera output, as well as a *Position Setting* pad.

Note: You must be logged into the camera before changing settings or else the operation will fail.

Adding a Preset

1. Use the directional pad to move the camera view. Use the center "home" button to return the camera to the default zeroed view.
2. Once the camera reaches the point where a preset is desired, type a name into the **Preset Point Name** field.

3. Click the **Add a preset point** to add the preset to the list. Click **OK** exit the menu, or you may continue to add/delete additional presets.

Deleting a Preset

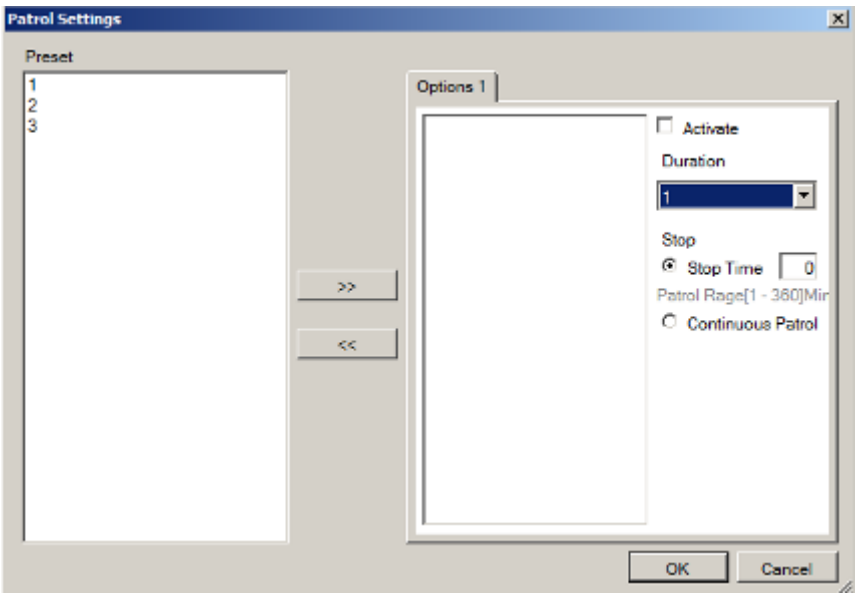
To delete a preset, simpy highlight the preset and click the **Delete** button. Click the **Yes** button to confirm deletion. Click **OK** exit the menu, or you may continue to add/delete additional presets.

Note: PTZ Preset Settings can also be configured by clicking ***Camera List*** > ***Camera Settings*** > ***Preset Settings*** in the SCC Console.

5.4.3. PTZ Patrol Settings

In cameras with PTZ functionality, one camera can be used to survey a large area. This can be done automatically using the patrol functionality. This function basically moves the camera between preset points in a fixed pattern. To configure camera patrol settings:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **PTZ Settings > Patrol Settings.**



Note: You must be logged into the camera before changing settings or else the operation will fail.

2. On the right side of the popup there will be a list of preset points that are defined for the camera. Use the >> button to add the points to the

patrol list in the order that they are to be viewed. Points can also be removed by highlighting them and clicking on the **<<** button.

3. Select the length of time the camera will dwell at each preset point before continuing from the **Dwelling Time (Sec)** dropdown.
4. Select one of the following:
   - **Stop Time** – The camera will stop the number of minutes specified in the box between patrol sessions.
   - **Never Stop** – The camera will not stop between patrol sessions.
5. Click the **Active** button to activate the patrol list.
6. Click the **OK** button to save the patrol list and exit the popup.

Note: PTZ Patrol Settings can also be configured by clicking ***Camera List*** > ***Camera Settings*** > ***Patrol Settings*** in the SCC Console.

5.5. PTZ Controls

Cameras equipped with Pan-Tilt-Zoom functionality can be controlled directly within the SCC client software. These controls can be found in the *Live View Control* window within the live view screen.

Note: (1) The camera to be controlled must be selected by highlighting it (clicking its output window) in the main view window. (2) Joystick can also be used for PTZ control. Please refer to *Server Setup* > *General Tasks* > *Joysticks* for more details.

5.5.1. Directional Pad

Pan and Tilt

The pan and tilt functionalities can be controlled with the directional pad.

Clicking the right or left arrow will pan the camera by one step in the direction clicked. Clicking the up or down arrow will tilt the camera by one step in the direction clicked. Clicking diagonal arrows will combine the pan and tilt action of the adjacent arrows.

Zoom

The zoom on a camera can be controlled with the + and – buttons located inside the direction pad. Pressing the + button will increase zoom distance by 1 step. Pressing the - button will decrease zoom distance by one step.

5.5.2. Functional Buttons

Speed

Auto Pan Speed – The speed which the camera will pan between the mechanical stops when the **Auto Pan** function is activated.

Pan Speed – The distance the camera will pan to each side.

Tilt Speed - The distance the camera will tilt up and down.

Zoom Speed - The distance the camera will zoom near or far.

Focus Speed - The amount the camera will focus forward or backward.

Home

One position can be set as the Home position. Click on Home button to go to the Home position. Clicking on the Home button will re-center the camera.

Preset

The camera may have preconfigured viewpoints, or presets configured. To switch to one of these presets, click the **Preset** button and select the preset.

Adding a Preset

You must first be logged into the camera to add a preset. To add a preset using the PTZ controls:

1. Pan, tilt, zoom, and focus to the desired preset position.
2. Click the **Preset** button and select **Add Preset**.
3. Type a name into the **Preset Name** field. Click **OK** to add the preset.

Deleting a Preset

You must first be logged into the camera. To delete a preset using the PTZ controls:

1. Pan to the the preset.
2. Click the Preset button and select Delete Preset Point.
3. Click the Yes button to confirm deletion.

Start Auto Pan

The camera will pan between the mechanical stops when the **Auto Pan** function is activated.

Stop Auto Pan

The camera will stop auto pan between the mechanical stops when the **Auto Pan** function is inactivated.

Focus

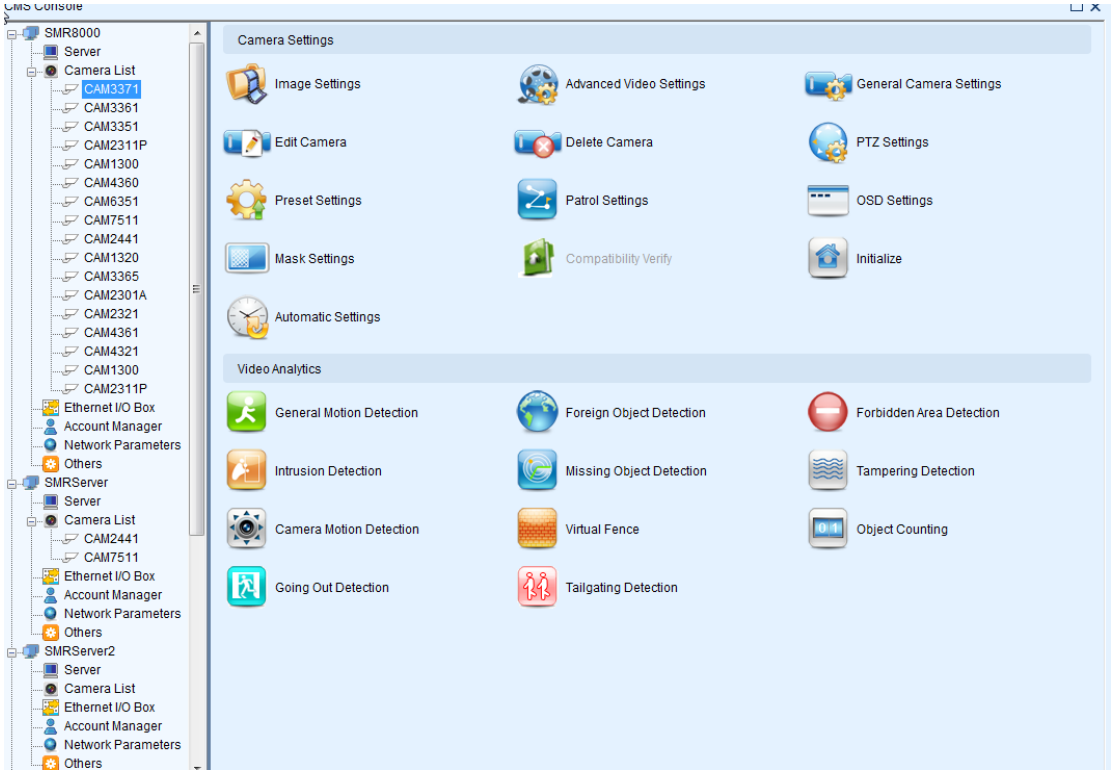
The focus on a camera can be controlled with the + and - buttons located beside the *Focus* box. Pressing the + button will increase focus distance by 1 step. Pressing the - button will decrease focus distance by one step.

Chapter 6. Alarms and Events

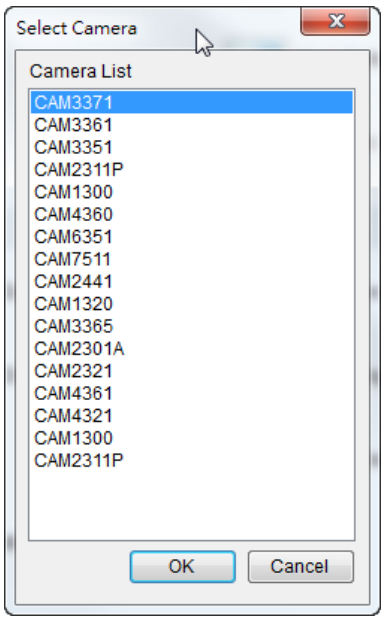
This section will guide you through the setup of VI detection and digital Inputs for detecting alarm conditions, the setup of digital outputs and alarm popups and notifications, as well as the setup of alarm rules and schedules.

6.1. Camera VI Detection Settings

Go to the setup page and the SCC Console page will come out. Click on the camera you'd like to set VI detections for on the camera list and you will see the following page.

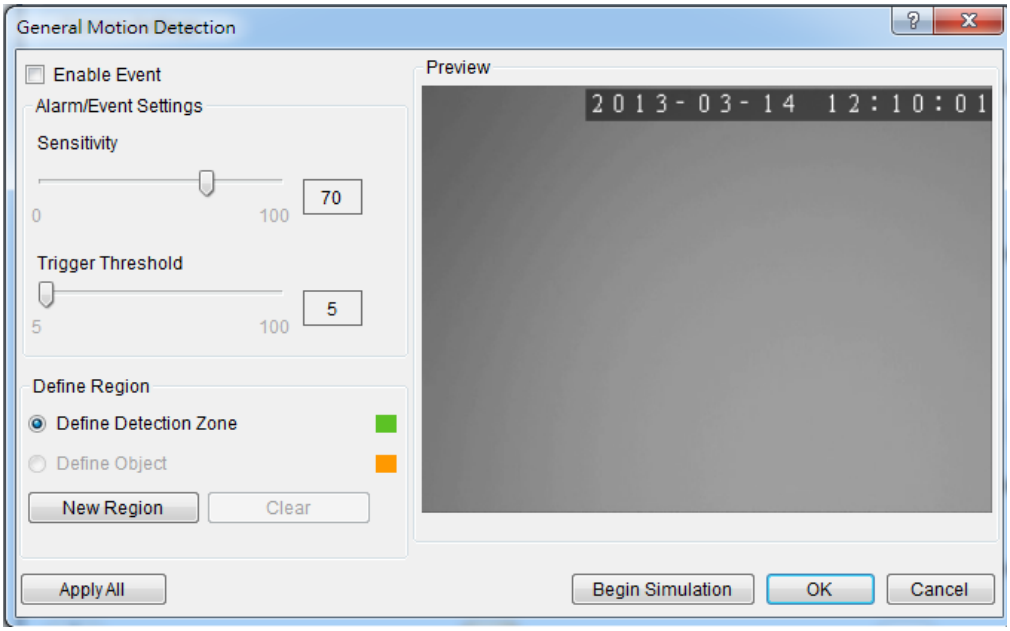


Or click on the Camera List to see the Video Analytics first and to specify the camera later after selecting any detection from this page.



6.1.1. General Motion Detection

Automatically detect the moving target entering the security area. When it moves, an alarm will be triggered.



Note: General Motion Detection can also be configured by clicking ***Camera List*** > ***Video Analytics*** > ***General Motion Detection*** in the SCC Console.

Configuring and Editing Detection Windows

1. Right-click the camera entry in the *Device Browser*, and click **VI Settings** > **General Motion Detection**.
2. If a new window is desired, click the **New Region** button to create a new window. Up to 3 detection windows can be set for each camera. The current window will be highlighted with a red border.
3. Click and drag the white dots along window border of a window to resize or reshape the window.
4. Click the interior of a window to drag it to the desired position.
5. Adjust the sliders: (Settings will be applied to all existing windows)

   - **Sensitivity** – Adjusts window sensitivity from 0 (low) to 100 (high).
   - **Trigger Threshold -** Adjusts the amount of change allowed before and event is triggered.

6. Click **OK** to save the changes and exit the popup.

Testing Detection Windows

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > General Motion Detection** option.
2. Click the **Begin Simulation** button enable test detection. During testing a red border will appear around any moving objects detected.
3. Click **End Simulation** to end the simulation.
4. Click **OK** to exit the popup.

Deleting a Detection Window

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > General Motion Detection** option.
2. Highlight an existing detection window.
3. Click the **Clear** button to delete the window.
4. Click **OK** to save the changes and exit the popup.

Enabling or Disabling a Detection

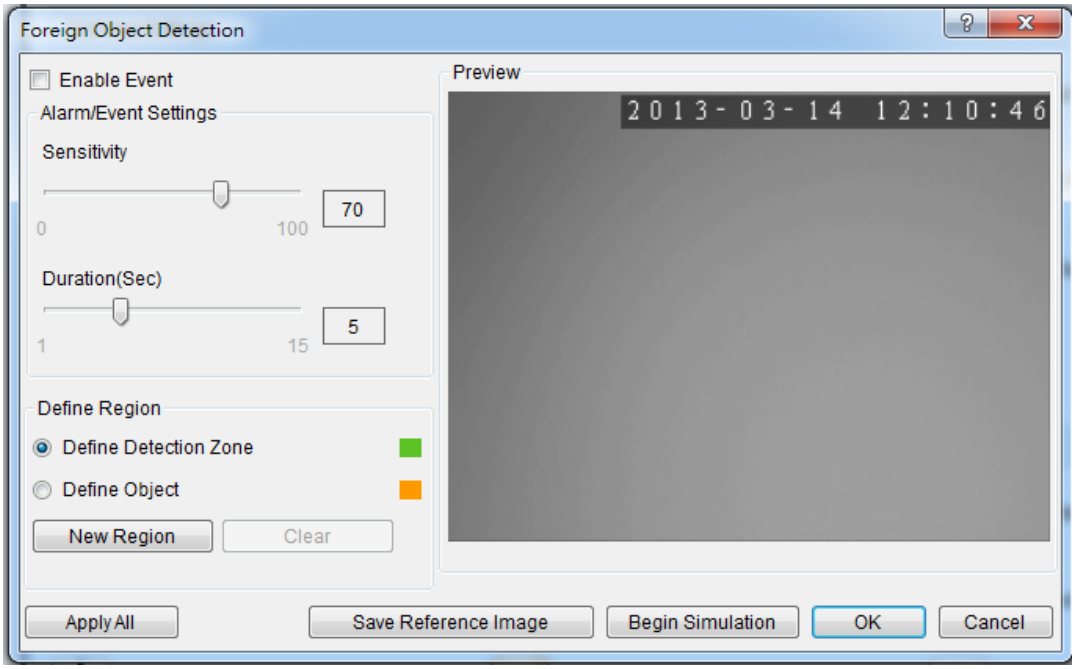
1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > General Motion Detection** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

Opening the Help File

The help file for General Motion Detection can be attached by clicking the icon on the upper right corner of the window.

6.1.2. Foreign Object Detection

Foreign object detection involves using the software to analyze a video feed and detect objects that do not belong.



Note: Foreign Object Detection can also be configured by clicking ***Camera List*** > ***Video Analytics*** > ***Foreign Object Detection*** in the SCC Console.

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right-click the camera entry in the *Device Browser*, and click **VI Settings** > **Foreign Object Detection**.
2. If a new window is desired, select **Define Detection Zone** and click the **New Region** button to create a new window. Up to 3 detection windows can be set for each camera. The current window will be highlighted with a red border.
3. Click and drag the white dots along window border of a window to resize or reshape the window.
4. Click the interior of a window to drag it to the desired position.
5. If an object size has not yet been defined, select **Define Object** and click the **New Region** button to create an object box.

6. Click and drag the corners of the object box to define the minimum size of objects that will be detected.

7. Adjust the sliders: (Settings will be applied to all existing windows)

   - **Sensitivity** – Adjusts window sensitivity from 0 (low) to 100 (high).
   - **Duration** - Adjusts the amount of time before an object triggers an event.

Click **OK** to save the changes and exit the popup.

Testing Detection Windows

To test a detection window:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > Foreign Object Detection** option.
2. Click the **Begin Simulation** button enable test detection. During testing a red border will appear around any foreign objects detected.
3. Click **End Simulation** to end the simulation.
4. Click **OK** to exit the popup.

Deleting a Detection Window

To delete a new detection window:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > Foreign Object Detection** option.
2. Highlight an existing detection window.
3. Click the **Clear** button to delete the window.
4. Click **OK** to save the changes and exit the popup.

Enabling or Disabling a Detection

To enable or disable the detection functions:

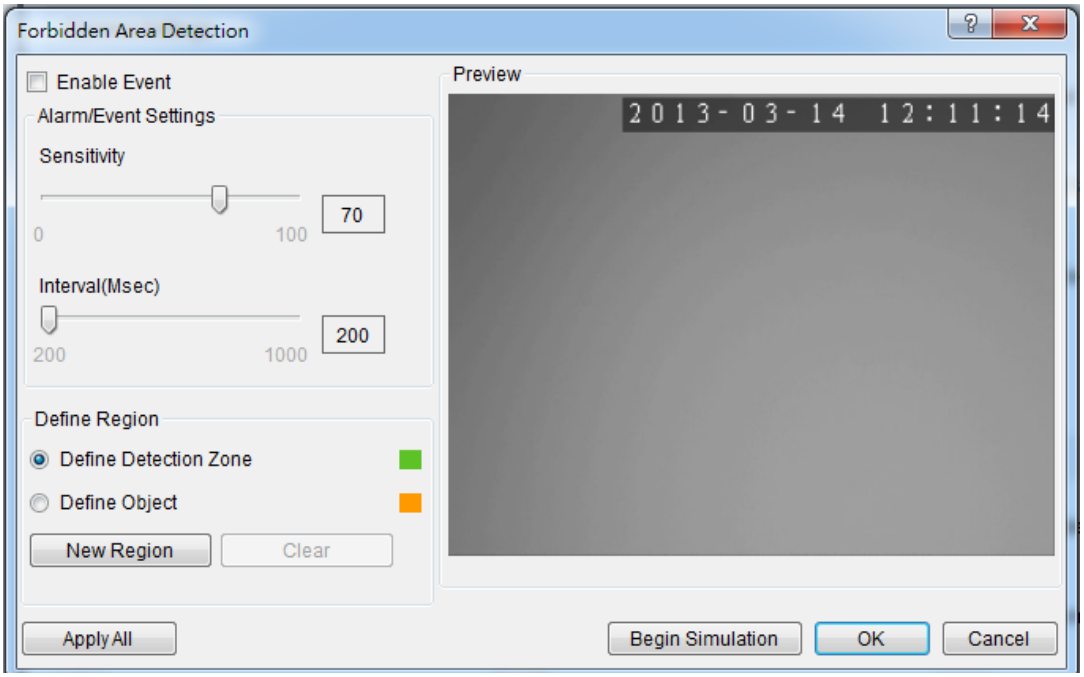
1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > Foreign Object Detection** option.

2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click OK to save the changes and exit the popup. Opening the Help File

The help file for Foreign Object Detection can be attached by clicking the icon on the upper right corner of the window.

6.1.3. Forbidden Area Detection

Forbidden area detection involves using the software to analyze the video feed and immediately detect any object in specified areas.



Note: Forbidden Area Detection can also be configured by clicking ***Camera List*** > ***Video Analytics*** > ***Forbidden Area Detection*** in the SCC Console.

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right-click the camera entry in the *Device Browser*, and click **VI Settings > Forbidden Area Detection**.
2. If a new window is desired, select **Define Detection Zone** and click the **New Region** button to create a new window. Up to 3 detection windows can be set for each camera. The current window will be highlighted with a red border.
3. Click and drag the white dots along window border of a window to resize or reshape the window.
4. Click the interior of a window to drag it to the desired position.
5. If an object size has not yet been defined, select **Define Object** and click the **New Region** button to create an object box.

6. Click and drag the corners of the object box to define the minimum size of objects that will be detected.
7. Adjust the sliders: (Settings will be applied to all existing windows)
    - **Sensitivity** - Adjusts window sensitivity from 0 (low) to 100 (high).
    - **Interval -** Adjusts how much time between each check of the forbidden area.
8. Click **OK** to save the changes and exit the popup.

Testing Detection Windows

To test a detection window:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > Forbidden Area Detection** option.
2. Click the **Begin Simulation** button enable test detection. During testing a red border will appear around any objects detected in the forbidden area.
3. Click **End Simulation** to end the simulation.
4. Click **OK** to exit the popup.

Deleting a Detection Window

To delete a new detection window:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > Forbidden Area Detection** option.
2. Highlight an existing detection window.
3. Click the **Clear** button to delete the window.
4. Click **OK** to save the changes and exit the popup.

Enabling or Disabling a Detection

To enable or disable the detection functions:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > Forbidden Area Detection** option.

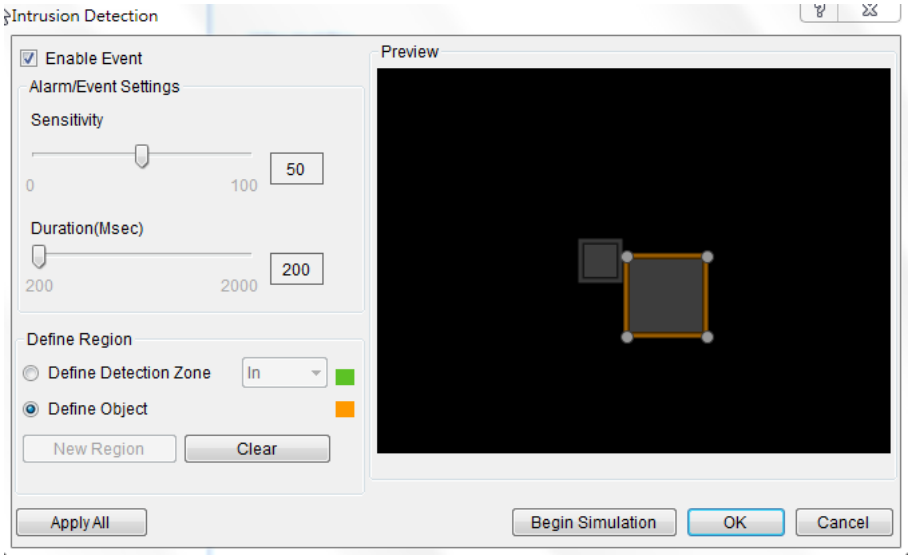
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

Opening the Help File

The help file for Forbidden Area Detection can be attached by clicking the icon on the upper right corner of the window.

6.1.4. Intrusion Detection

Intrusion detection involves using the software to analyze the video feed and detect intrusion larger than a certain size.



Note: Intrusion Detection can also be configured by clicking ***Camera List*** > ***Video Analytics*** > ***Intrusion Detection*** in the SCC Console.

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right-click the camera entry in the *Device Browser*, and click **VI Settings** > **Intrusion Detection**.
2. If a new window is desired, select **Define Detection Zone** and click the **New Region** button to create a new window. Up to 3 detection windows can be set for each camera. The current window will be highlighted with a red border.
3. Click and drag the white dots along window border of a window to resize or reshape the window.
4. Click the interior of a window to drag it to the desired position.
5. If an object size has not yet been defined, select **Define Object** and click the **New Region** button to create an object box.
6. Click and drag the corners of the object box to define the minimum size of the intrusion that will be detected.

7. Adjust the sliders: (Settings will be applied to all existing windows)

    - **Sensitivity** - Adjusts window sensitivity from 0 (low) to 100 (high).
    - **Duration (Sec)** - Adjusts how much time an object is missing before an event is triggered.

8. Click **OK** to save the changes and exit the popup.

Testing Detection Windows

To test a detection window:

1. Right-click the camera entry in the Device Browser, then highlight and click the **VI Settings > Intrusion Detection** option.
2. Click the **Begin Simulation** button enable test detection. During testing a red border will appear if any intrusion found.
3. Click **End Simulation** to end the simulation.
4. Click **OK** to exit the popup.

Deleting a Detection Window

To delete a new detection window:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > Intrusion Detection** option.
2. Highlight an existing detection window.
3. Click the **Clear** button to delete the window.
4. Click **OK** to save the changes and exit the popup.

Enabling or Disabling a Detection

To enable or disable the detection functions:

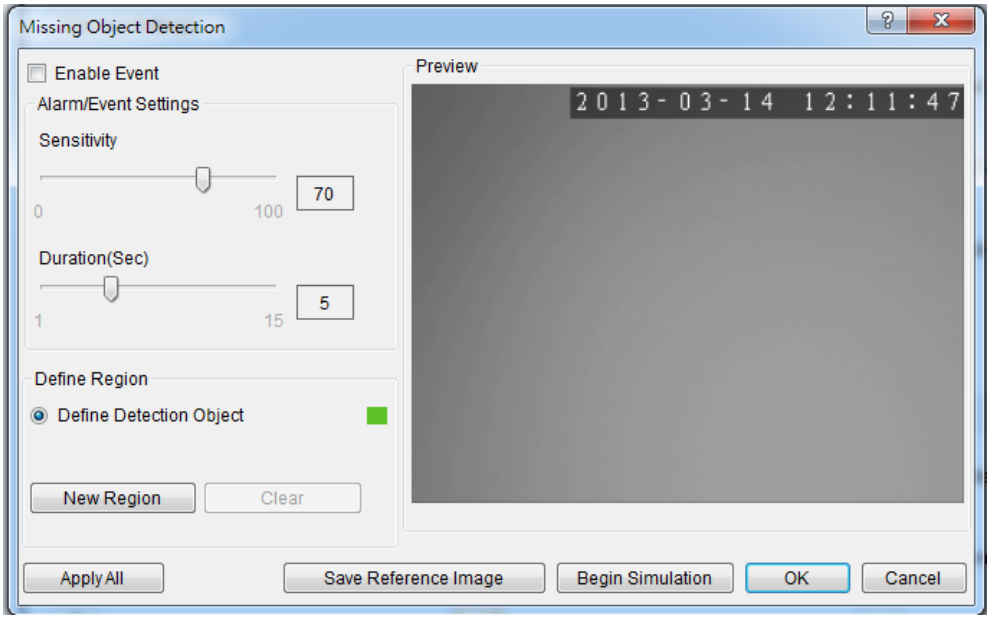
1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > Intrusion Detection** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

Opening the Help File

The help file for Intrusion Detection can be attached by clicking the icon on the upper right corner of the window.

6.1.5. Missing Object Detection

Missing object detection involves using the software to analyze the video feed and detect missing objects larger than a certain size.



Note: Missing Object Detection can also be configured by clicking ***Camera List*** > ***Video Analytics*** > ***Missing Object Detection*** in the SCC Console.

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right-click the camera entry in the *Device Browser*, and click **VI Settings** > **Missing Object Detection**.
2. If a new window is desired, select **Define Detection Zone** and click the **New Region** button to create a new window. Up to 3 detection windows can be set for each camera. The current window will be highlighted with a red border.
3. Click and drag the white dots along window border of a window to resize or reshape the window.
4. Click the interior of a window to drag it to the desired position.
5. If an object size has not yet been defined, select **Define Object** and click the **New Region** button to create an object box.
6. Click and drag the corners of the object box to define the minimum size of the missing objects that will be detected.

7. Adjust the sliders: (Settings will be applied to all existing windows)

    - **Sensitivity** - Adjusts window sensitivity from 0 (low) to 100 (high).
    - **Duration (Sec)** - Adjusts how much time an object is missing before an event is triggered.

8. Click **OK** to save the changes and exit the popup.

Testing Detection Windows

To test a detection window:

1. Right-click the camera entry in the Device Browser, then highlight and click the **VI Settings > Missing Object Detection** option.
2. Click the **Begin Simulation** button enable test detection. During testing a red border will appear if a object goes missing.
3. Click **End Simulation** to end the simulation.
4. Click **OK** to exit the popup.

Deleting a Detection Window

To delete a new detection window:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > Missing Object Detection** option.
2. Highlight an existing detection window.
3. Click the **Clear** button to delete the window.
4. Click **OK** to save the changes and exit the popup.

Enabling or Disabling a Detection

To enable or disable the detection functions:

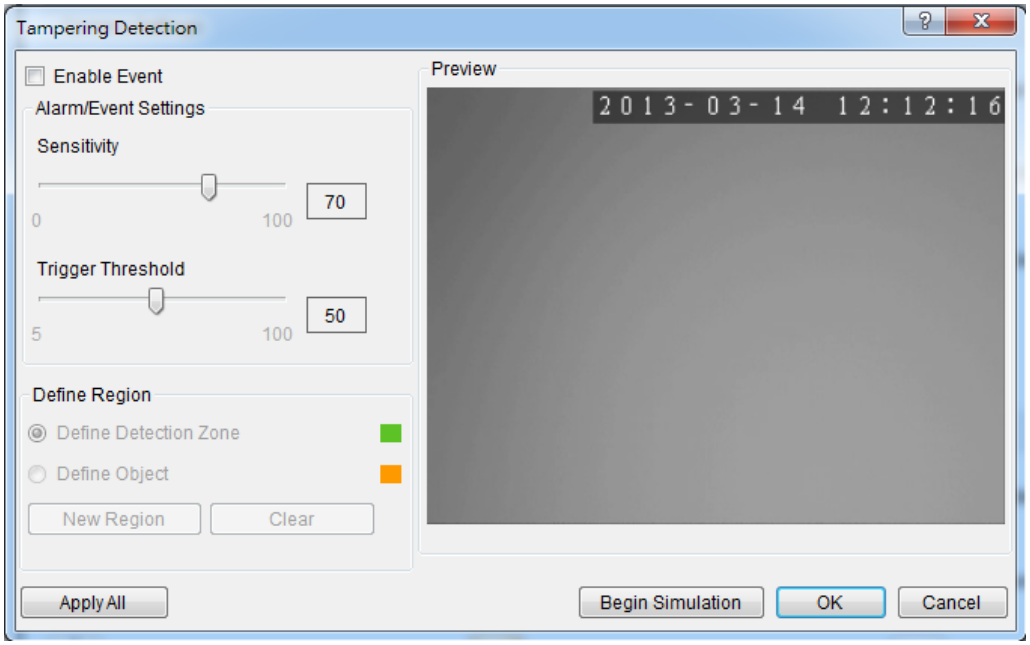
1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > Missing Object Detection** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

Opening the Help File

The help file for Missing Object Detection can be attached by clicking the icon on the upper right corner of the window.

6.1.6. Tampering Detection

Tampering detection involves using the software to determine when the camera has been improperly moved or redirected.



Note: Tampering Detection can also be configured by clicking ***Camera List*** > ***Video Analytics*** > ***Tampering Detection*** in the SCC Console.

Configuring Tampering Detection

To configure a new detection window:

1. Right-click the camera entry in the *Device Browser*, and click **VI Settings** > **Tampering Detection**.
2. Adjust the sliders:
   - **Sensitivity** - Adjusts window sensitivity from 0 (low) to 100 (high).
   - **Trigger Threshold** - Adjusts the amount of change allowed before an event is triggered.
3. Click **OK** to save the changes and exit the popup.

Testing Tampering Detection

To test a detection window:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > Tampering Detection** option.
2. Click the **Begin Simulation** button enable test detection. During testing a red border if tampering is detected.
3. Click **End Simulation** to end the simulation.
4. Click **OK** to exit the popup.

Enabling or Disabling a Detection

To enable or disable the detection functions:

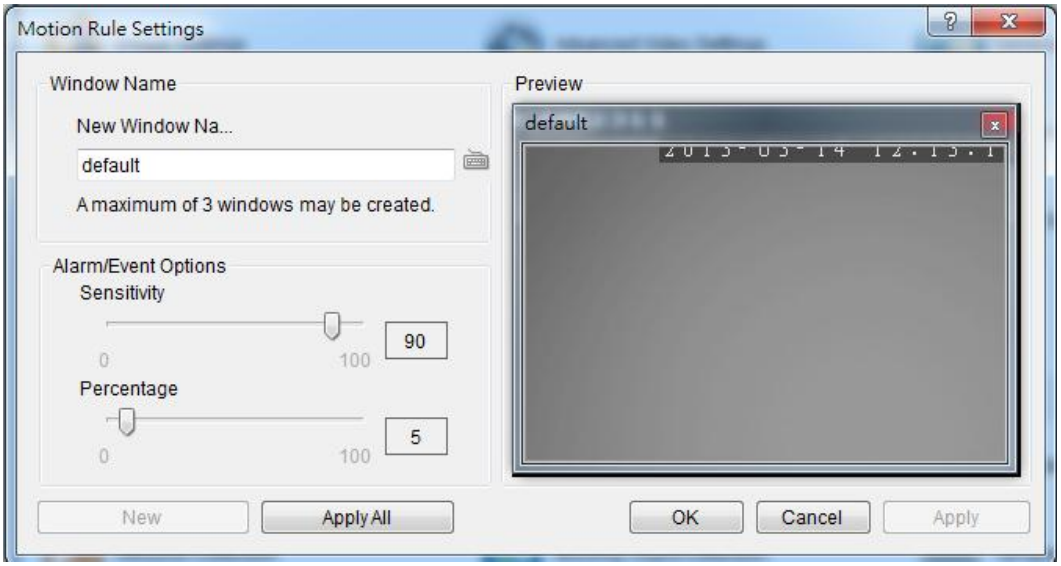
1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > Tampering Detection** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

Opening the Help File

The help file for Tampering Detection can be attached by clicking the icon on the upper right corner of the window.

6.1.7. Camera Motion Detection

Camera motion detection involves using the camera hardware to analyze the video feed and detect motion in specified areas.



Note: Camera Motion Detection can also be configured by clicking ***Camera List*** > ***Video Analytics*** > ***Camera Motion Detection*** in the SCC Console.

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right click the camera entry in the *Device Browser*, and click **VI Settings** > **Camera Motion Detection**.

Note: You must be logged into the camera before changing settings or else the operation will fail.

2. If a new window is desired, enter a name in the **New Window Name** field and click the **New** button. Up to 3 detection windows can be set for each camera. The current window will be highlighted.
3. Click and drag the window border of a window to resize or reshape the window.
4. Click the interior of a window to drag it to the desired position.
5. Adjust the sliders: (Settings will be applied to all existing windows)

   - **Sensitivity** - Adjusts window sensitivity from 0 (low) to 100 (high).

- **Percentage -** Adjusts the amount of the window that must change before an event is triggered.

6. Click **Apply** to save the changes and **OK** to exit the popup.

Deleting a Detection Window

To delete a new detection window:

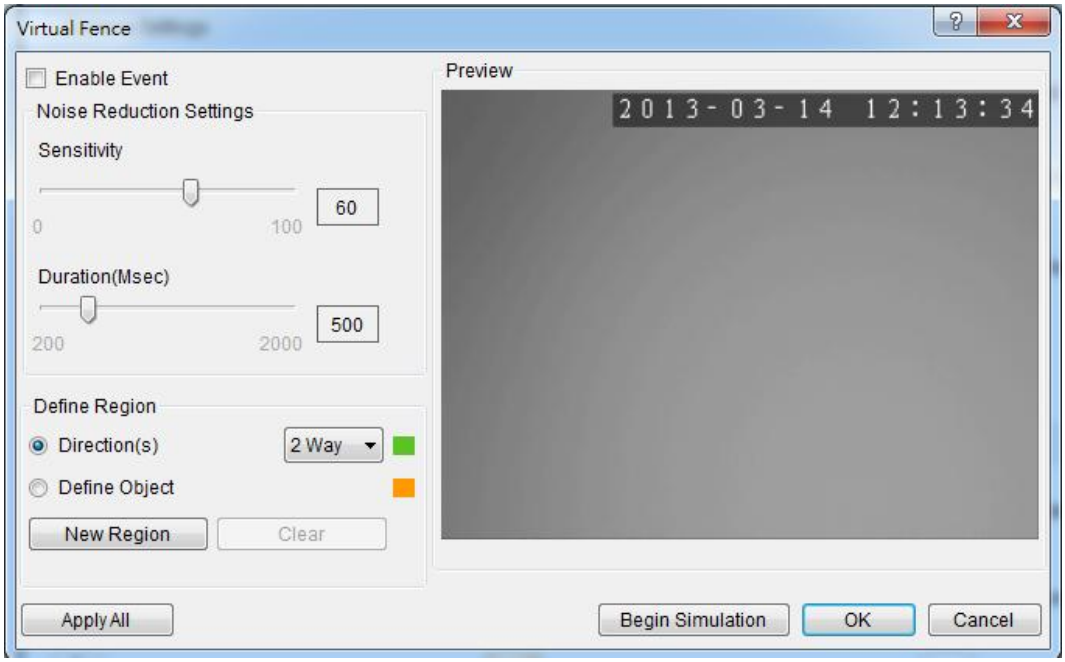
1. Right click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > Camera Motion Detection** option.
2. Click the **X** at the top right corner of the window to delete the window.
3. Click **OK** to save the changes and exit the popup.

Opening the Help File

The help file for Camera Motion Detection can be attached by clicking the icon on the upper right corner of the window.

6.1.8. Virtual Fence

Virtual fence involves using the software to create a fence-crossing detection of the demanding object.



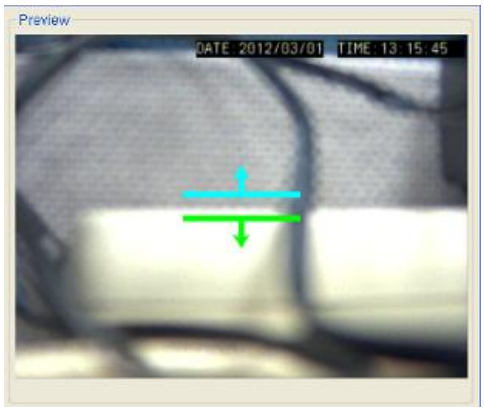
Note: Virtual Fence can also be configured by clicking ***Camera List*** > ***Video Analytics*** > ***Virtual Fence*** in the SCC Console.

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right-click the camera entry in the *Device Browser*, and click **VI Settings > Virtual Fence**.

   If a new window is desired, select **Directions** and click the **New Region** button to create a new window. The current window will be highlighted with a one/two-way arrow (blue means “in”, green means “out”).



2. Click and drag the white arrows along the window border around the one/two-way arrow to resize the space between the fences/adjust the length of the fences.
3. Turn the window border with the orange arrow to change the directions of the fences.
4. If an object size has not yet been defined, select **Define Object** and click the **New Region** button to create an object box.
5. Click and drag the corners of the object box to define the minimum size of the fence-crossing objects that will be detected.
6. Adjust the sliders: (Settings will be applied to all existing windows)

    - **Sensitivity** - Adjusts window sensitivity from 0 (low) to 100 (high).
    - **Duration (Sec)** - Adjusts how much time between each check for the fence-crossing.

7. Click **OK** to save the changes and exit the popup.

Testing Detection Windows

To test a detection window:

1. Right-click the camera entry in the Device Browser, then highlight and click the **VI Settings > Virtual Fence** option.
2. Click the **Begin Simulation** button enable test detection. During testing a red border will appear if a object goes missing.
3. Click **End Simulation** to end the simulation.
4. Click **OK** to exit the popup.

Deleting a Detection Window

To delete a new detection window:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > Virtual Fence** option.
2. Highlight an existing detection window.
3. Click the **Clear** button to delete the window.

4. Click **OK** to save the changes and exit the popup.

Enabling or Disabling a Detection

To enable or disable the detection functions:

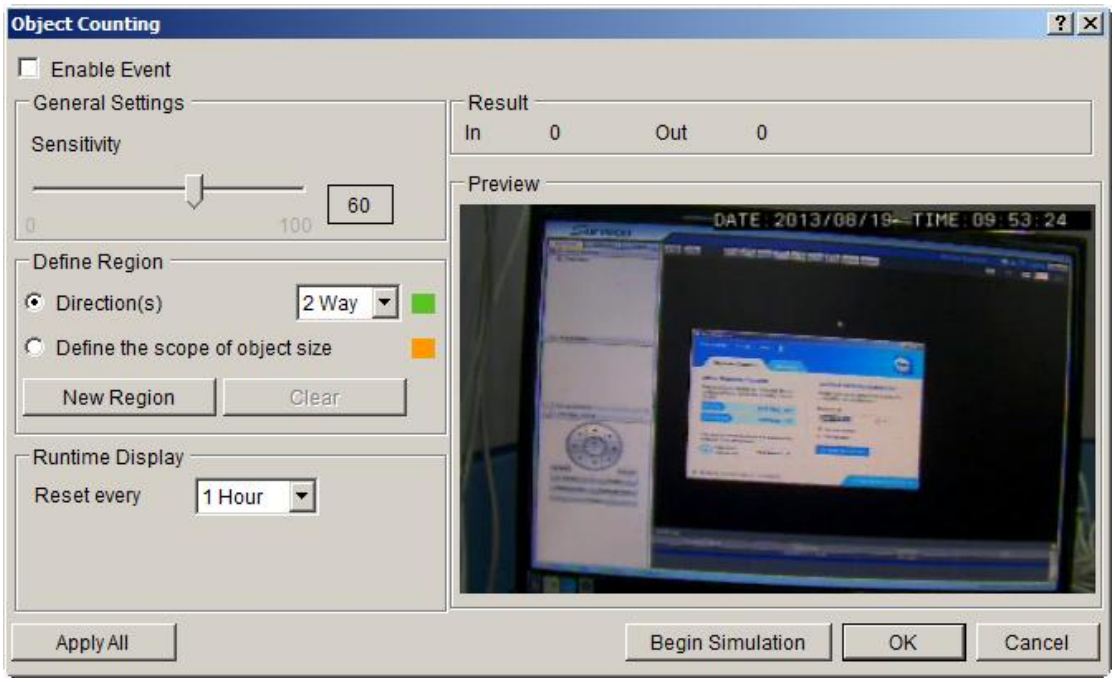
1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > Virtual Fence** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

Opening the Help File

The help file for Virtual Fence can be attached by clicking the icon on the upper right corner of the window.

6.1.9. Object Counting

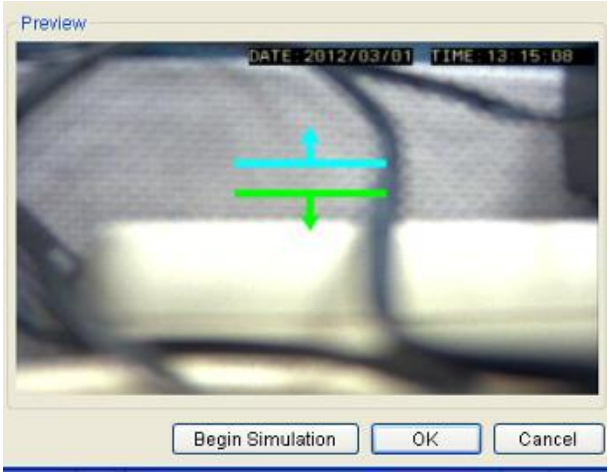
Object counting involves using the camera to count demanding object crossing the fences.



Configuring and Editing Detection Windows

To configure a new detection window:

1. Right-click the camera entry in the *Device Browser*, and click **VI Settings > Object Counting**.
2. If a new window is desired, select **Directions** and click the **New Region** button to create a new window. The current window will be highlighted with a one/two-way arrow (blue means “in”, green means “out”).



3. Click and drag the white arrows along the window border around the one/two-way arrow to resize the space between the fences/adjust the length of the fences.
4. Turn the window border with the orange arrow to change the directions of the fences.
5. If an object size has not yet been defined, select **Define the scope of object size** and click the **New Region** button to create an object box.

Note: (1) Only people will be counted after Define the scope of object size is selected. (2) It is recommended that the object size is smaller than 1/4 of the live view screen.

6. Click and drag the corners of the object box to define the minimum size of the fence-crossing objects that will be detected.
7. Adjust the sliders: (Settings will be applied to all existing windows)

   - **Sensitivity** - Adjusts window sensitivity from 0 (low) to 100 (high).

8. The update interval can be set as 5min, 10min, 15min, 30 min and 1 hour in **Runtime Display**.
9. Click **OK** to save the changes and exit the popup.

Testing Detection Windows

To test a detection window:

1. Right-click the camera entry in the Device Browser, then highlight and click the **VI Settings > Object Counting** option.
2. Click the **Begin Simulation** button enable test detection. During testing a red border will appear if a object goes missing.
3. Click **End Simulation** to end the simulation.
4. Click **OK** to exit the popup.

Deleting a Detection Window

To delete a new detection window:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > Object Counting** option.
2. Highlight an existing detection window.
3. Click the **Clear** button to delete the window.
4. Click **OK** to save the changes and exit the popup.

Enabling or Disabling a Detection

To enable or disable the detection functions:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > Object Counting** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

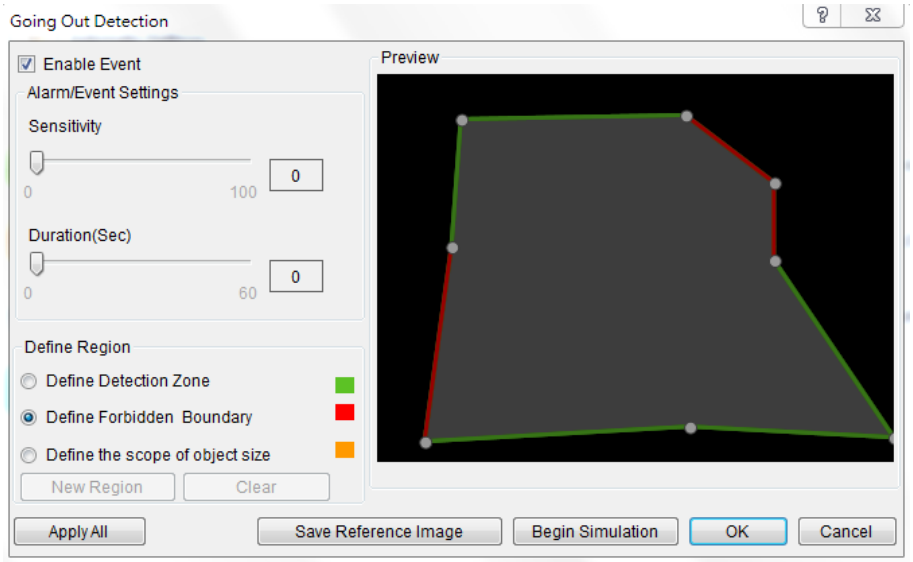
Note: (1) Object Counting can also be configured by clicking ***Camera List > Video Analytics > Object Counting*** in the SCC Console. (2) The statistical results for object counting can be seen by choosing the *Counting* Tab in the View Log Windows. Please refer to *Log for Object Counting* section for more details.

Opening the Help File

The help file for Object Counting can be attached by clicking the icon on the upper right corner of the window.

6.1.10. Going Out Detection

Going Out detection involves using the software to analyze the video feed and detect a going-out object crossing over the restricted area.



Note: Going Out Detection can also be configured by clicking ***Camera List*** > ***Video Analytics*** > ***Going Out Detection*** in the SCC Console.

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right-click the camera entry in the *Device Browser*, and click **VI Settings > Going Out Detection**.
2. If a new window is desired, select Define Detection Zone and click the New Region button to create a new window. Only 1 detection window can be set for each camera.
3. Click and drag the white dots along window border of a window to resize or reshape the window.
4. Click the interior of a window to mark the restricted line; once clicked, the clicked line will turn red. The red lines are the boundaries. Up to 8 boundaries can be set.
5. If an object size has not yet been defined, select Define Object and click the New Region button to create an object box.
6. Click and drag the corners of the object box to define the minimum size of the objects that will be detected.

7. Adjust the sliders: (Settings will be applied to all existing windows)

    - Sensitivity – Adjusts window sensitivity from 0 (low) to 100 (high).
    - Duration (Sec) - Adjusts how much time an object is missing before an event is triggered.

8. Click OK to save the changes and exit the popup.

Testing Detection Windows

To test a detection window:

1. Right-click the camera entry in the Device Browser, then highlight and click the **VI Settings > Going Out Detection** option.
2. Click the **Begin Simulation** button enable test detection. During testing a red border will appear if any intrusion found.
3. Click **End Simulation** to end the simulation.
4. Click **OK** to exit the popup.

Deleting a Detection Window

To delete a new detection window:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > Going Out Detection** option.
2. Highlight an existing detection window.
3. Click the **Clear** button to delete the window.
4. Click **OK** to save the changes and exit the popup.

Enabling or Disabling a Detection

To enable or disable the detection functions:

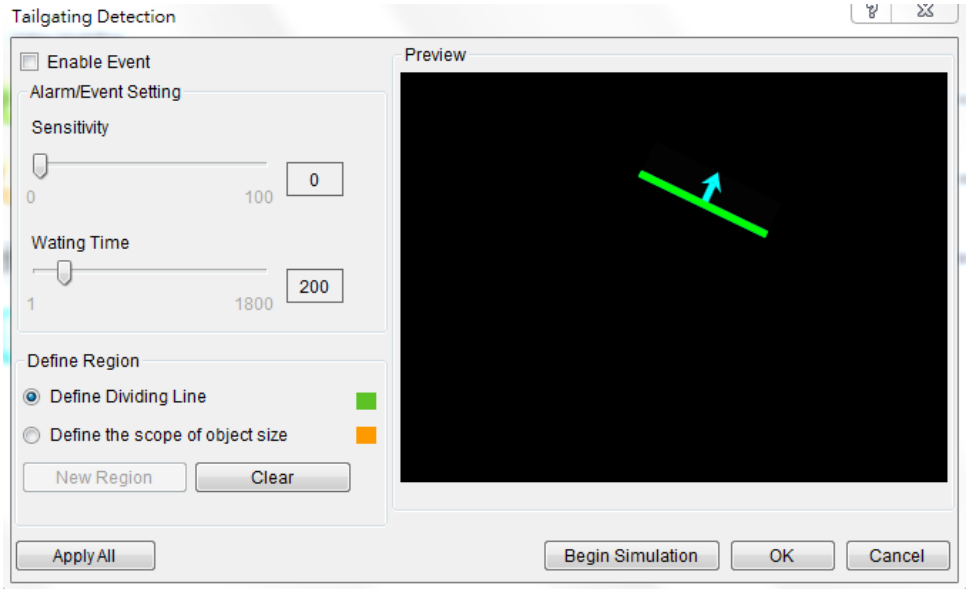
1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > Going Out Detection** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

Opening the Help File

The help file for Going Out Detection can be attached by clicking the icon on the upper right corner of the window.

6.1.11. Tailgating Detection

Tailgating detection involves using the software to analyze the video feed and detect a tailgating object crossing over the restricted area.



Note: Tailgating Detection can also be configured by clicking ***Camera List*** > ***Video Analytics*** > ***Tailgating Detection*** in the SCC Console.

Configuring and Editing Detection Windows

To configure a new detection window:

1. Right-click the camera entry in the *Device Browser*, and click **VI Settings > Tailgating Detection**.
2. If a new window is desired, select Define Dividing Line and click the New Region button to create a new dividing line. Only 1 dividing line can be set for each camera.
3. Click and drag the created dividing line to the desire position and direction.
4. If an object size has not yet been defined, select Define Object and click the New Region button to create an object box.
5. Click and drag the corners of the object box to define the minimum size of the objects that will be detected.
6. Adjust the sliders: (Settings will be applied to all existing windows)

    - Sensitivity – Adjusts window sensitivity from 0 (low) to 100 (high).

- Waiting Time (Sec) - Adjusts how much time an object is tailgating before an event is triggered.

7. Click OK to save the changes and exit the popup.

Testing Detection Windows

To test a detection window:

1. Right-click the camera entry in the Device Browser, then highlight and click the **VI Settings > Tailgating Detection** option.
2. Click the **Begin Simulation** button enable test detection. During testing a red border will appear if any intrusion found.
3. Click **End Simulation** to end the simulation.
4. Click **OK** to exit the popup.

Deleting a Dividing LIne

To delete a new dividing line:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > Tailgating Detection** option.
2. Highlight the dividing line.
3. Click the **Clear** button to delete the line.
4. Click **OK** to save the changes and exit the popup.

Enabling or Disabling a Detection

To enable or disable the detection functions:

1. Right-click the camera entry in the *Device Browser*, then highlight and click the **VI Settings > Tailgating Detection** option.
2. Check the **Enable Event** box to enable detection, or uncheck the box to disable detection.
3. Click **OK** to save the changes and exit the popup.

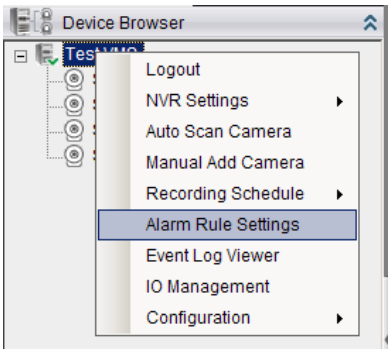
Opening the Help File

The help file for Tailgating Detection can be attached by clicking the icon on the upper right corner of the window.

6.2. Alarm Rules

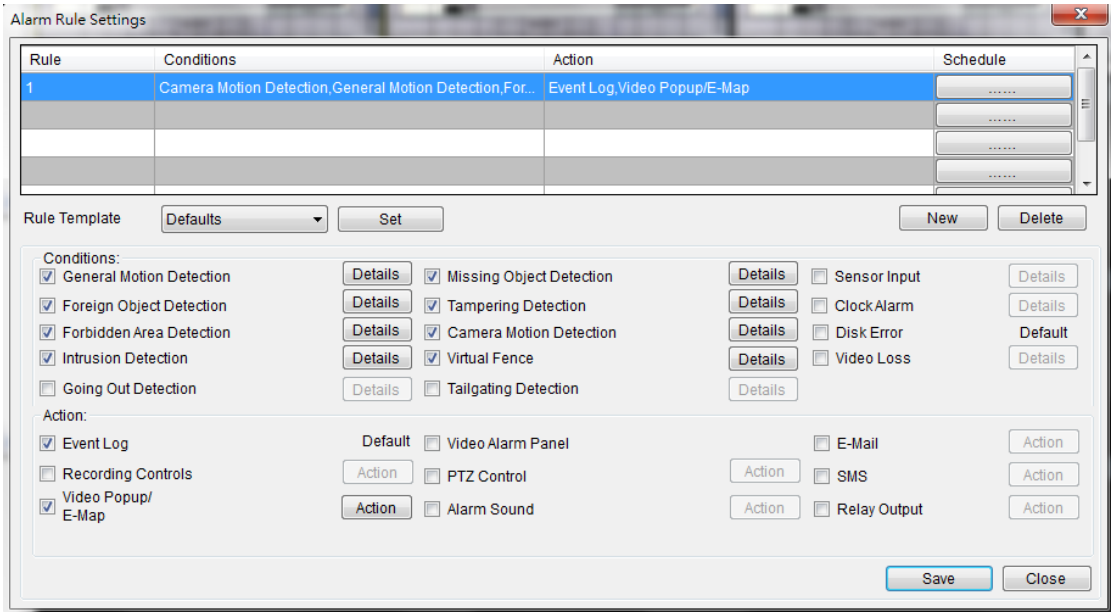
SCC Client provides robust alarm handling features.

To access these features right-click the Server entry and then highlight and click the **Alarm Rule Settings** option.



Note: Alarm Rule Settings can also be accessed by clicking ***Server > General Tasks > Alarm Rule Settings*** or ***Server Entry > Common Tasks > Common Server Tasks > Alarm Rule Settings*** in the SCC Console.

In the alarm rule settings, you can combine the alarm trigger conditions with action items such as event notification, video recording, and/or camera movements. Multiple alarm rules can be created using the following elements:



1. **Rule**: A short description. For example, “east –fence intrusion detection” or “front entrance access control.”
2. **Condition**: Specifies triggering conditions such as Motion/Video loss/Sensor input/Clock Alarm, etc.

3. **Action**: Specifies the action to take when the alarm is triggered.
4. **Schedule**: Allows the user to schedule the application of specific Alarm rules. This is useful in cases such as applying rules to non-office hours.

6.2.1. Adding an Alarm Rule

1. Click the **New** button.
2. Enter a short description for the new rule in the **Add Rule** field.
3. Choose conditions and actions. Click the **…...** button in the description field to set up a schedule for the rule. These selections are described in the following sections.
4. Click the **Set** button to save the rule.

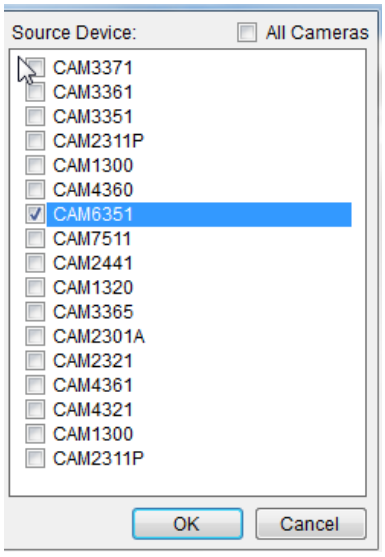
Alarm Conditions

The following alarm conditions can be set to trigger the alarm:

Detections

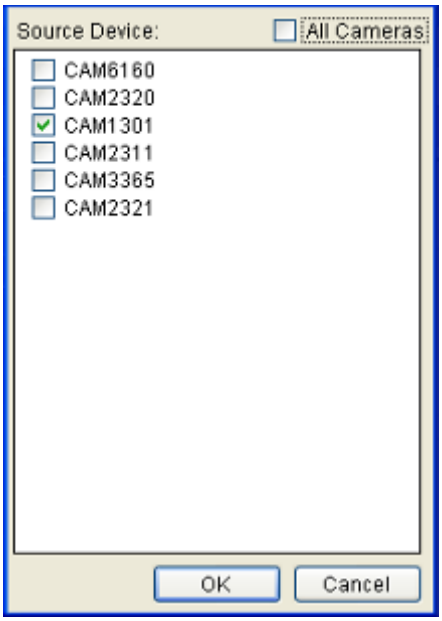
When configuring a camera, a detection area can be specified. After the detection area is specified, detection can be activated and an alarm handling scheme configured in this menu.

Clicking on the **Detail** button will pull up a menu listing all the devices with General Motion Detection active.



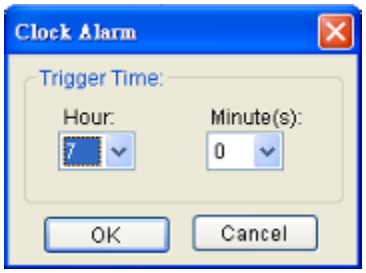
Sensor Input

The alarm is triggered by a sensor input. For example this may include doorway entry sensors that are connected to the camera system. Clicking on the Detail button will pull up the *Sensor Input Settings* menu, listing all the cameras. From this menu, click the checkboxes next to the cameras that will be used to trigger the Alarm. Optionally, check the **All Cameras** check box to use all the cameras available. Click the **OK** button to exit the menu.



Clock Alarm

When a preset time is reached, the alarm is triggered. The Clock Alarm is triggered only on the day it is configured. Clicking on the **Detail** button will pull up the *Clock Alarm* menu.



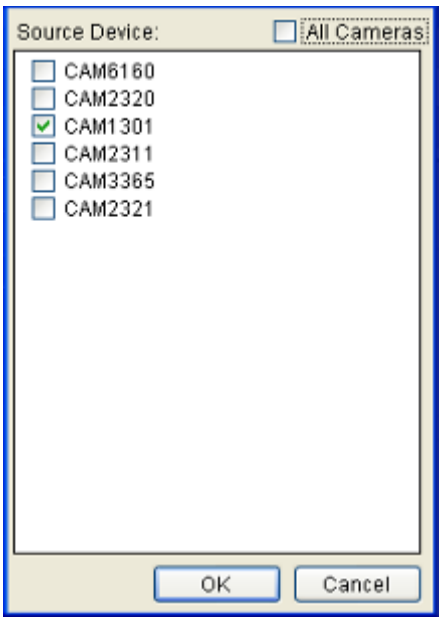
From this popup select the hour and minute the alarm will be triggered. Click the **OK** button to exit the menu.

Disk Error

The alarm is triggered when a disk drive failure occurs.

Video Loss

When video input is lost, the alarm is triggered. Clicking on the **Details** button will pull up the *Video Loss Settings* menu, listing all the cameras. From this menu, click the checkboxes next to the cameras that will be used to trigger the Alarm. Optionally, check the **All Cameras** check box to use all the cameras available. Click the **OK** button to exit the menu.



Alarm Actions

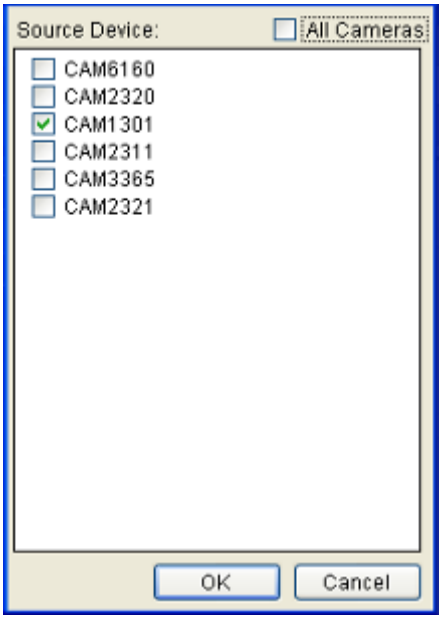
The following alarm actions can be taken when the alarm is triggered:

Event Log

The system issues event messages when the alarm is triggered.

Recording Controls / Video Popup

When the alarm is triggered, the system records video onto the storage. Clicking on the **Action** button will pull up the *Recording Settings* menu.



Use the checkboxes within to select cameras that will be recorded. Optionally, check the **All Cameras** check box to use all the cameras available. Click the **OK** button to exit the menu.

E-Map

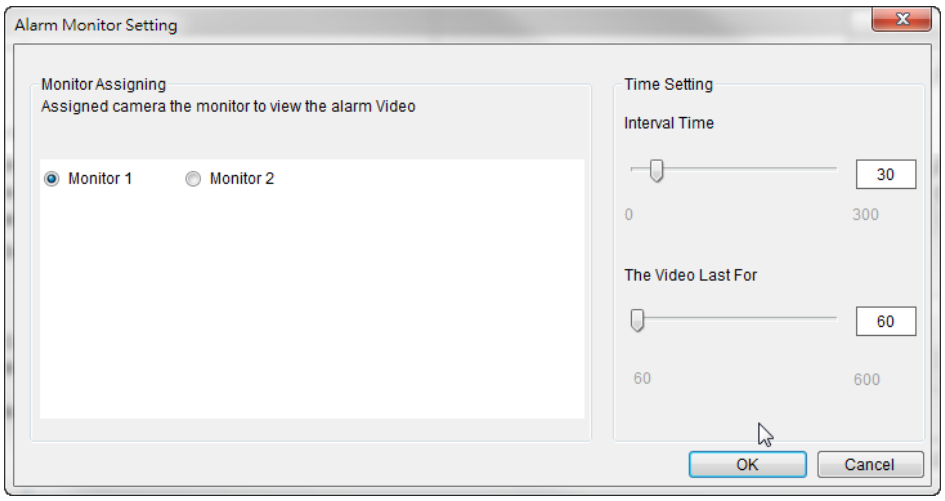
When the alarm is triggered, a popup video appears on the local client.

Clicking the **Action** button will pull up a menu.

Alarm Monitor

When there are more than 2 monitors are being used, you can assign one monitor to display popup notification when any alarm is triggered.

Interval time and video duration can be further defined.

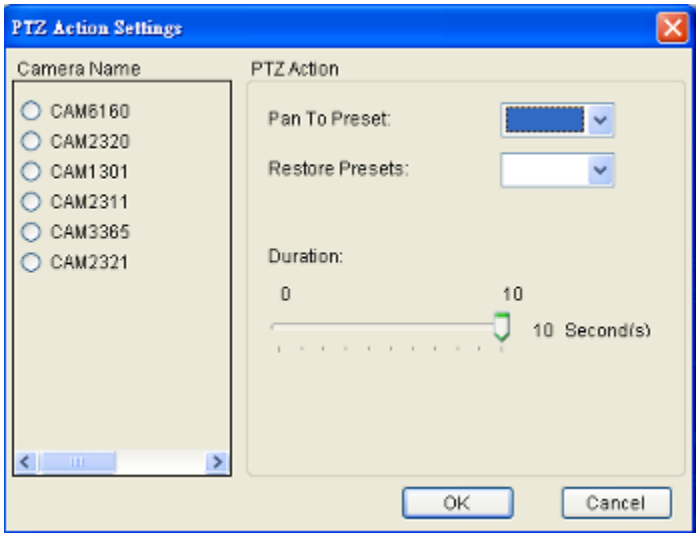


Video Alarm Panel

This will display the video feed thumbnail in the video alarm panel for review and playback.

PTZ Control

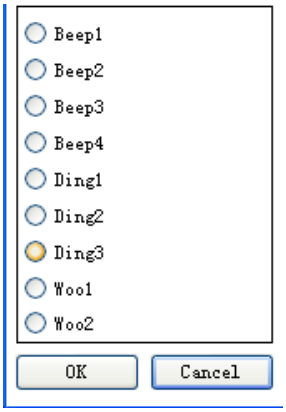
When the alarm is triggered, a Pan-Tilt-Zoom action can be set to slew the camera to a particular position. For example, clicking on the **Action** button brings up the *PTZ Action Settings* menu. In this menu:



1. Choose a camera from the list.
2. Select a preset point from the **Pan to Preset** dropdown that the camera will pan to.
3. Select the preset that the camera will return to from the **Restore Presets** dropdown.
4. Specify a duration that the camera will stay at the **Pan to Action** preset before returning to the **Restore to Preset** preset using the **Duration** slider. Click **Apply** to save the settings.
5. Click **OK** to exit the menu.

Alarm Sound

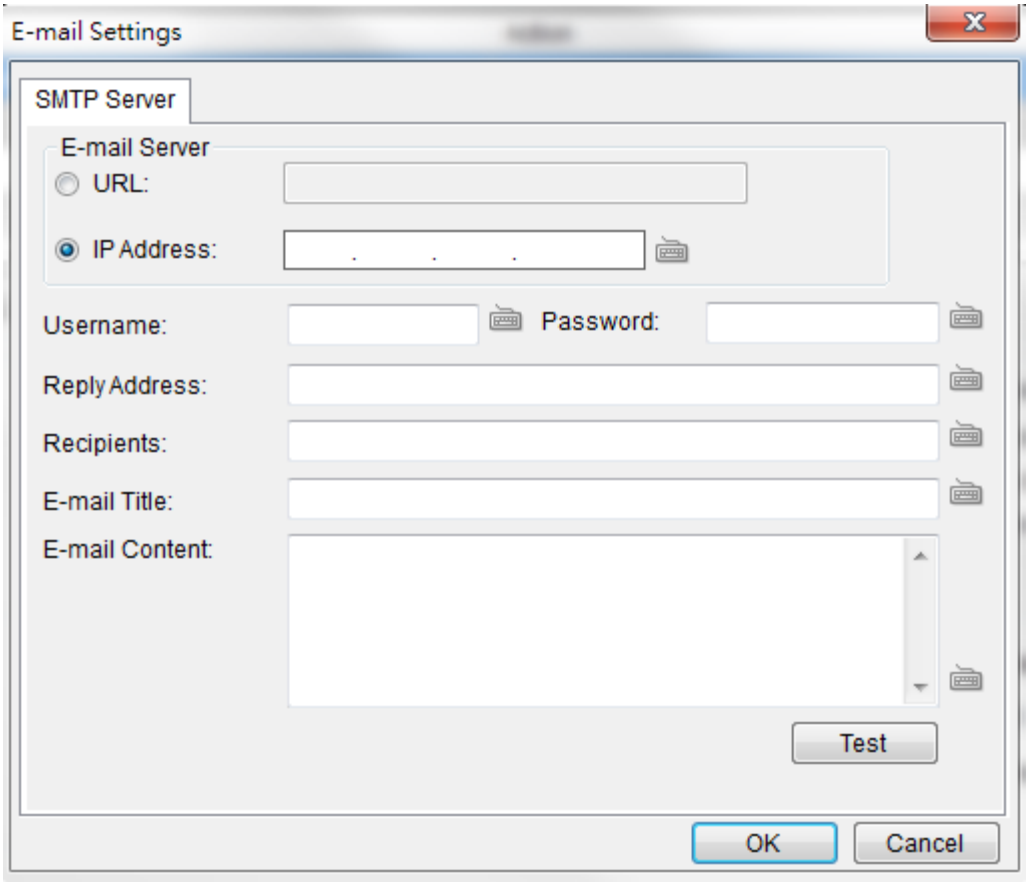
When the alarm is triggered, the system will play an audible alarm sound. Clicking on the **Action** button will pull up the *Warning Sound* menu, listing available sounds.



Choose a sound by clicking the radio box next to the desired sound. Click the **OK** button to exit the menu.

E-Mail

When the alarm is triggered, an E-Mail will be sent. Checking this option will bring up the *E-mail Settings* menu.



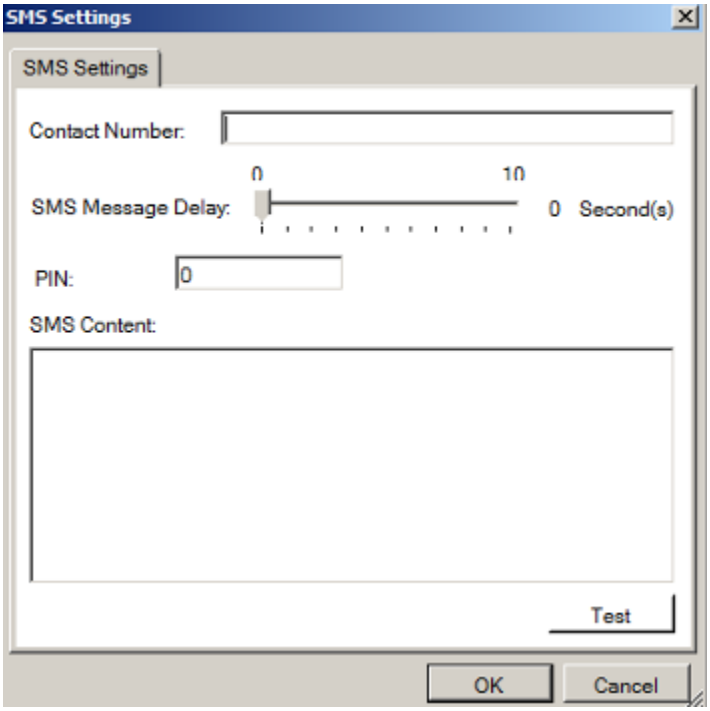
1. In the *SMTP Server* tab, under the *E-mail Server* heading, you may either enter the URL (such as smtp.abc.com) or IP address of the SMTP server that the Server will use to deliver E-mail notifications. The SMTP server configured here must support Unicode Transformation Format-8 (UTF-8) encoding.
2. Enter the user name for the Server email account in the **Username** field.
3. Enter the password for the Server email account in the **Password** field.
4. Enter a valid E-mail address in the **Reply Address** field. This address will be the default sender listed in E-mails sent from the Server.
5. Enter one or more E-mail addresses in the **Recipients**: field. These address(es) will receive notifications from the Server. Multiple addresses can be entered by separating individual addresses with semi -colons ";".
6. Enter the subject of your notification E-mails, e.g., Server-xxxsite1notification in the **E- Mail Title** field.
7. Enter a short message in the large field to describe the Server or a surveillance network.

8. **(Optional)** Click **Test** to send a test message to the E-mail addresses listed.

9. Click the **OK** button to exit E-mail settings.

SMS

When the alarm is triggered, an SMS message will be sent. Checking this option will bring up the *SMS Settings* menu.



Note: Drivers for supported GSM/GPRS modems have already been installed on the server. Currently, only the **WaveCOM-M1206B** is supported. Use COM1 on the Server to connect to a GSM modem.

1. In the **Contact Number** field, enter the phone numbers that will receive SMS notifications. Be sure to include the area code, e.g., “86”, in front of phone numbers. Use commas, “,” to separate individual phone numbers.

2. Use the slider bar to select a delay between the occurrence of an event and SMS message delivery.

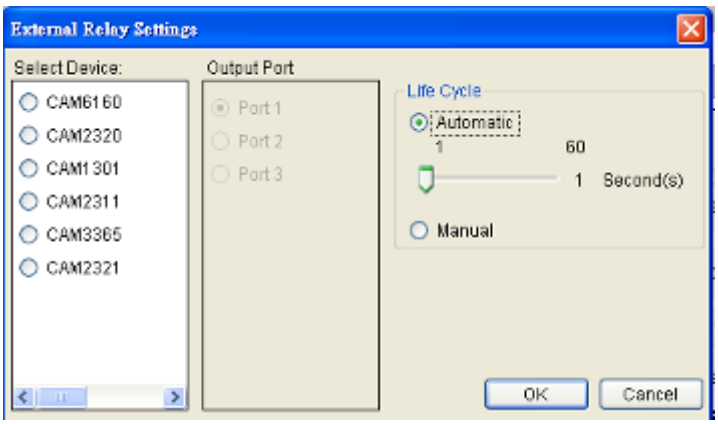
3. **(Optional)** If a SIM PIN is required, enter the PIN code in the **PIN** field. Note that applying incorrect PIN code may disable your SIM card.

Note: To change the PIN code, remove the SIM card from your GSM modem. Use a cell phone to change the PIN code and then re -install SIM card into the GSM modem. Changing PIN codes is not recommended because a configuration failure may disable your SIM card.

4. In the **SMS Content** field, type a simple description to include in the outgoing SMS messages
5. **(Optional)** Click **Test** to send a test message to the phone numbers listed.
6. Click the **Apply** button to apply the changes.
7. Click the **OK** button to exit SMS settings.

Relay Output

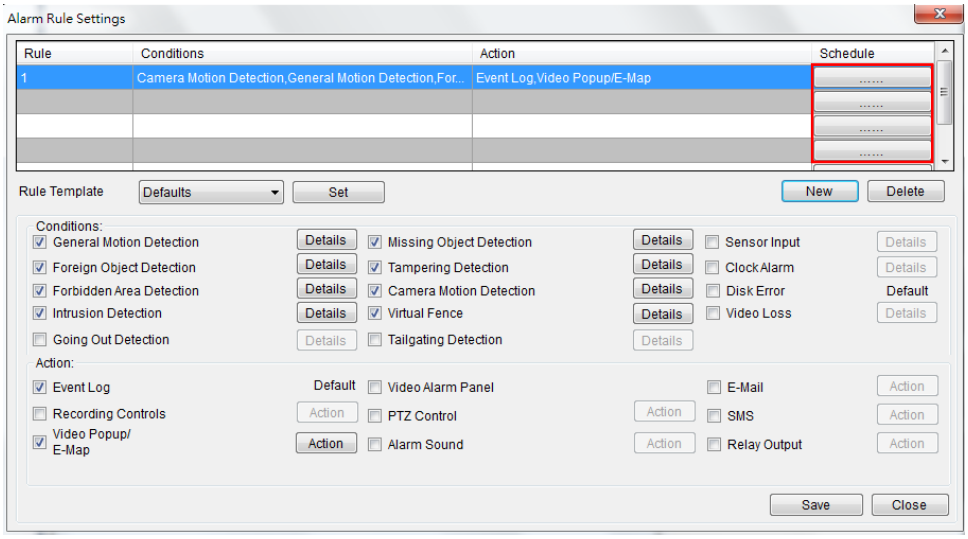
When the alarm is triggered, a signal will be relayed to an external source such as a light switch, siren, or other external link. Clicking on the **Action** button brings up the *External Relay Settings* menu. In this menu:

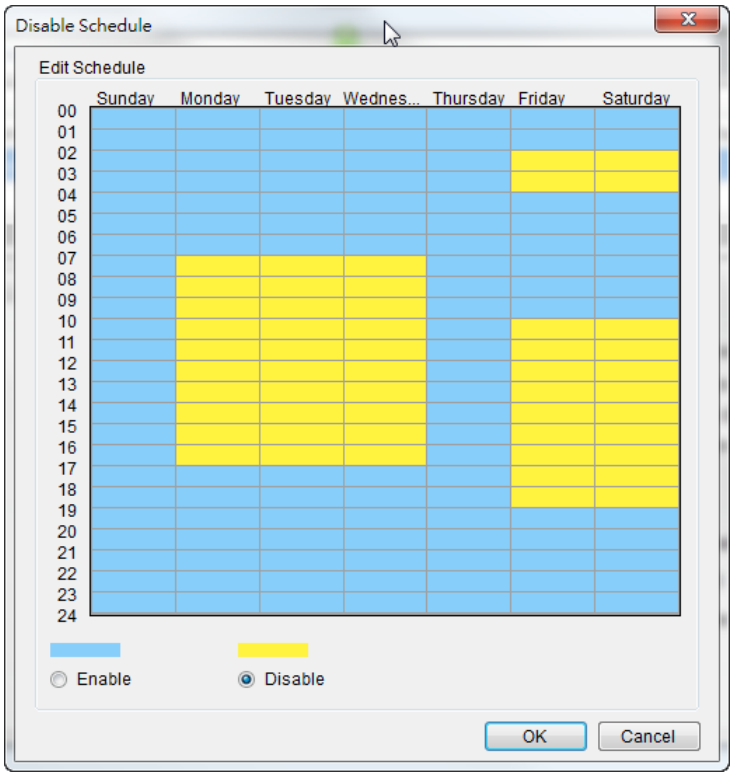


1. Choose a camera from list.
2. Select an output port to relay to.
3. Select output duration, from 0 to 60 seconds.
4. Click the **OK** button to exit the menu.

Alarm Scheduling

When the alarm is created, click the ……button located in the scheduling column of the alarm listing to bring up the *Alarm Rule Schedule* menu. This displays a table with the days of the week as the columns, and hours as the rows, allowing the user to schedule the alarm on exact hours.





From this menu, use the following steps to schedule the alarm:

1. Choose the rule that you wish to apply the schedule to.
2. Click the **Enable** or **Disable** button to bring up a "paintbrush."
3. Click the cursor on the table to "paint" in a schedule. You may click and drag to paint a wide area.

For example, if you wish to disable the alarm on Tuesday at 6pm, you would click the box Tuesday-18:00. Disabled time periods are highlighted in yellow.

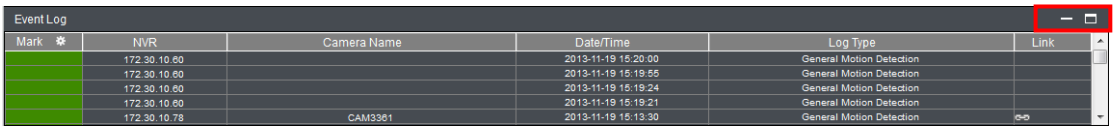
Click the **OK** button to apply the changes and exit the menu.

6.3. Alarms View and Notification

Alarm information is displayed in 3 different ways when in the live view mode.

6.3.1. Live View Event Log

Alarms are displayed is in the Event Log section of the live view screen. As alarms come in, they are displayed in this area. This area can be minimized or maximized using the double arrow at the upper right corner.



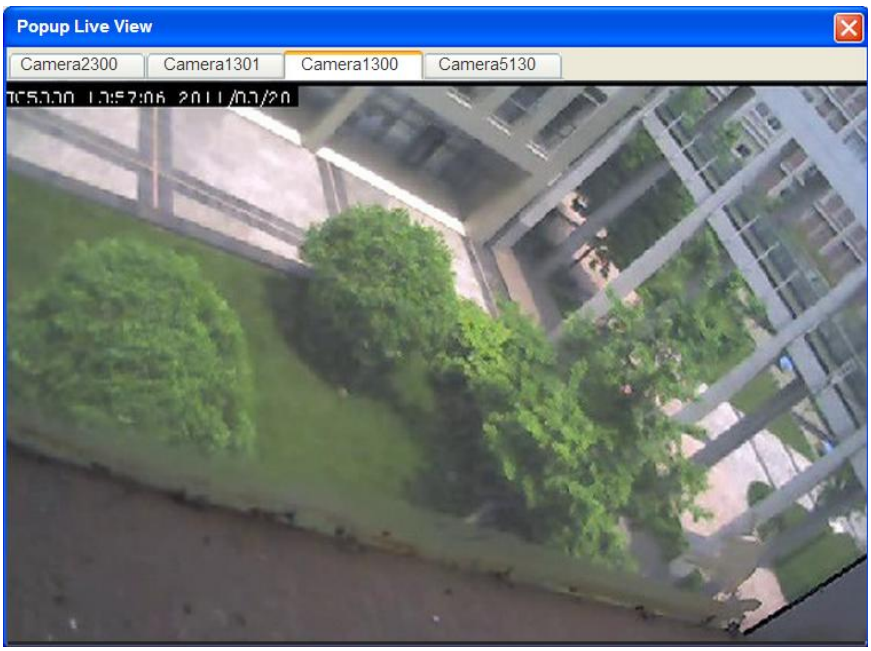
The Event Log displays the camera the alarm occurred on, the date, the alarm type, and if applicable a link to the live-view feed of the camera. Clicking on the link will open the camera's live-view in a popup.

1. **Mark*:** double click this item to further define the color bar shown on the Event Log.
2. **NVR:** the IP Address of the NVR
3. **Camera Name:** the camera being alarm-triggered
4. **Date/Time:** when the triggered event was taken place.
5. **Log Type:** alarm type
6. **Link:** clink the link can be directed to the playback to see the triggered moment.

6.3.2. Alarm Popups

Alarms can be configured to display a popup window when triggered.

Up to 4 windows can be popped up at the same time. If there's a fifth alarm occurs, the SCC will close the oldest popup window and show the new popup.



When the alarm is triggered the **Open Popup Window** button will flash red. When this occurs, clicking the button will open a popup.

The popup will display the alarm trigger condition, the camera that triggered the alarm as well as live feed from this camera, the time of the alarm, and a custom configurable message. Any additional popups can be viewed using the left and right arrows located below the video feed.

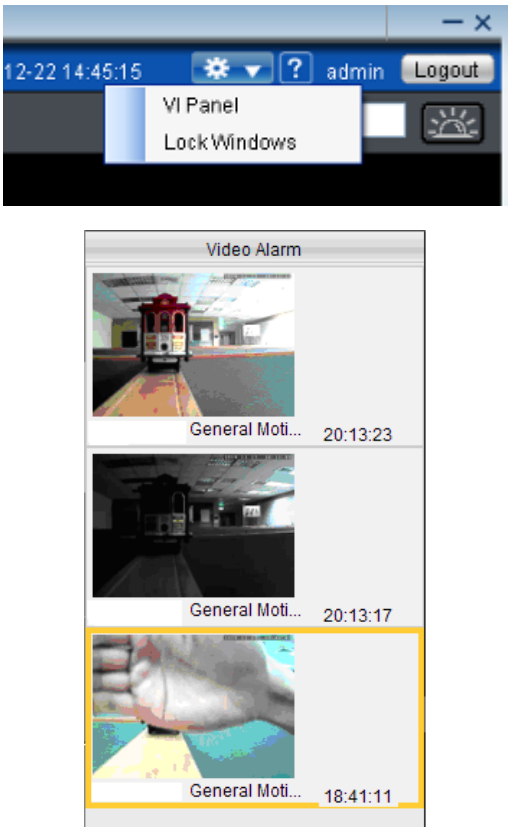
Setting Popup Sleep Time

A skip time, in which similar alarms will not trigger a popup for the camera in question, can be configured in the *Alarm Sleep Time* box. Using the drop-downs, specify the number of minutes and seconds of skip time. Click **Apply** to save your settings.

Clicking the **OK** button will close the window and save the sleep settings. Clicking the **Cancel** button will close the window without saving the sleep settings.

6.3.3. Video Panel

Alarms can be configured to display in the *Video Panel*, located to the left of the main viewing area. When an alarm configured in this manner is triggered, a thumbnail of the triggering event will be displayed in the panel, and actions can be taken from this panel.



Note: VI Panel functionality can also be enabled under ***Server*** > ***Other Tasks*** > ***VI Panel*** in the SCC Console.

Playback from Video Alarm Panel

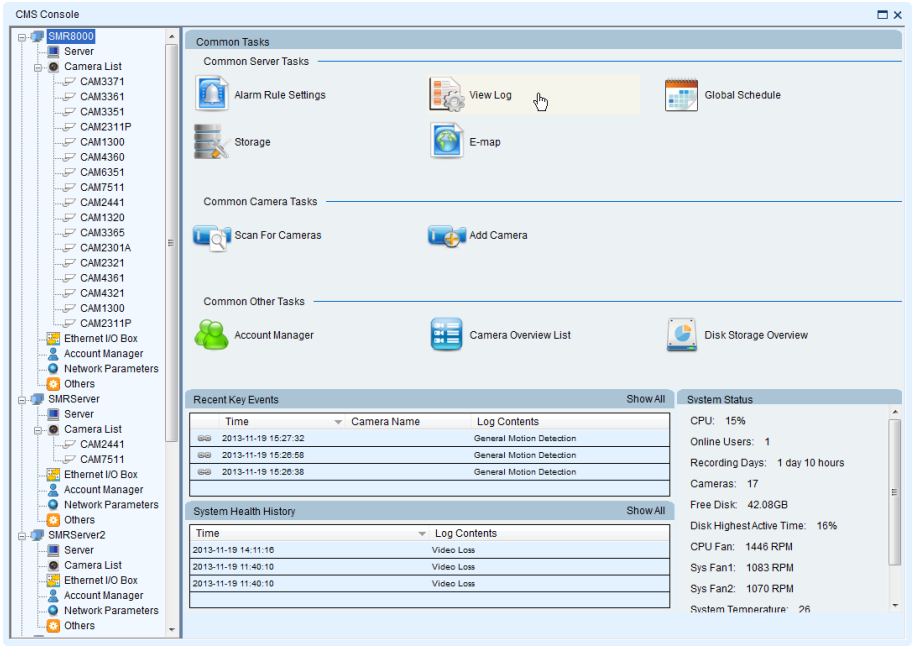
The server is configured to record up to 45 minutes of video after an alarm is triggered. To play back this video, right click the thumbnail and select **Play> [Time Length]**. A popup will open with the desired playback. Time lengths available are dependent on, and will not exceed the post-alarm recording time set in **Pre/Post Alarm Recording Settings**.

Tagging an Alarm Thumbnail

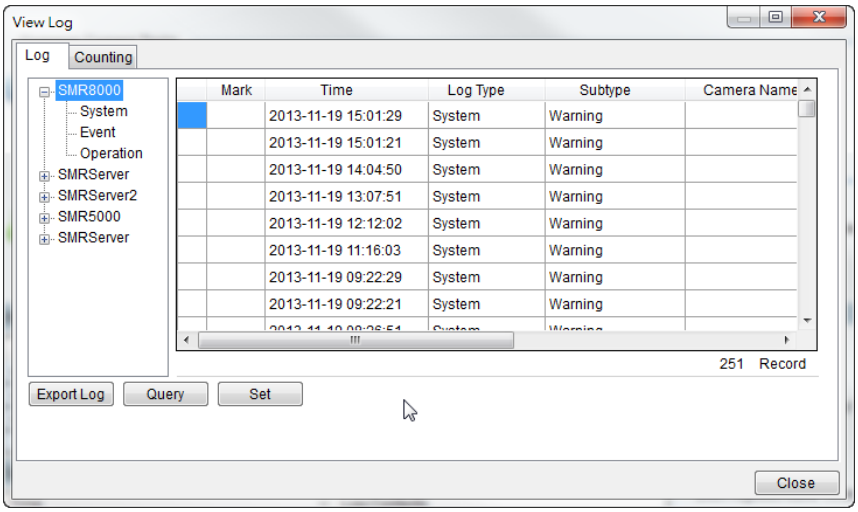
Another unique feature of alarms in the alarm panel, is that they can be tagged for future reference. To tag the alarm, right-click the thumbnail and select **Mark > [Label].** Labels available are dependent on system configurations, but the default labels are *Mark, Check, Clear, Suspicious.*

6.4. Event Log

The event log is a comprehensive repository of all the events that occur on the system. On the setup page, right-click the Server entry and choosing the **View Log** entry, the *View Log* window will display.



The log viewer displays events, split into three types, System events, which deal with individual modules, Camera events, which deal with cameras and operational events which deal with user accounts.



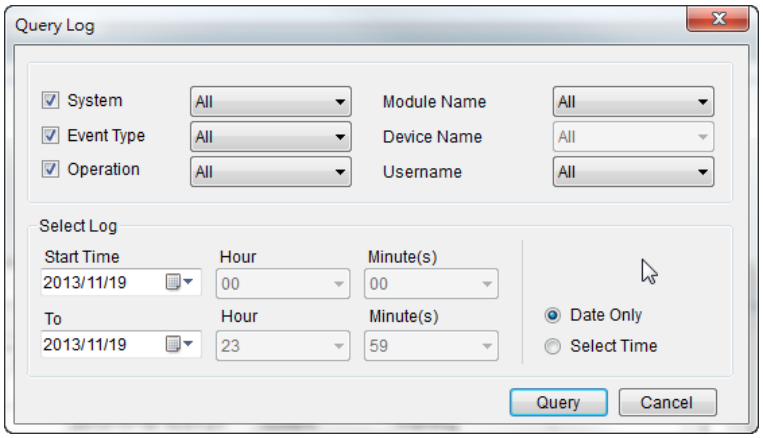
Note: Event Log can also be viewed by clicking ***Server Entry*** > ***Common Tasks*** > ***Common Server Tasks*** > ***View Log*** or ***Server*** > ***General Tasks*** > ***View Log*** in the SCC Console.

6.4.1. Exporting a Log

If log entries exist, they may be exported by clicking on the **Export Log** button at the bottom of the View *Log* screen. This will open a dialog box, which prompts the user to choose a location, and fill in a name for the saved log. Fill out the location and filename information and click **OK** to save the logfile.

6.4.2. Searching the Event Log

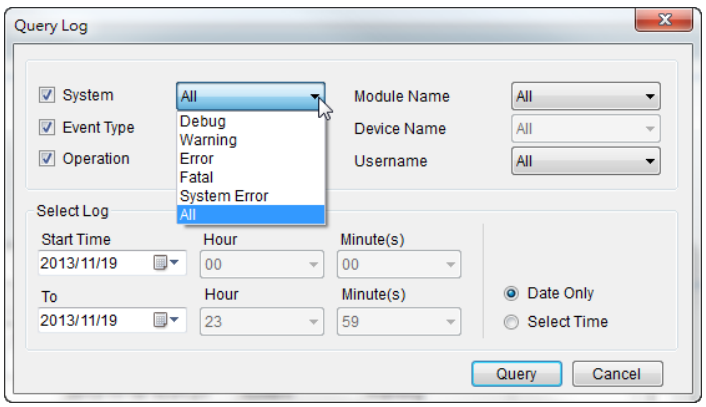
Within the *View Log* screen, click the **Query** button to bring up the *Query Log* dialog box.



Within this dialog, the user may choose to narrow the search to the three major event types by selecting the checkbox beside the event type:

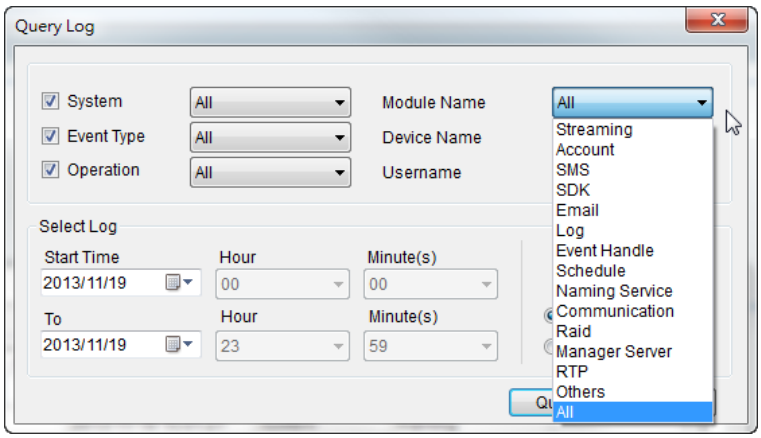
System Type

These are errors that occur within individual system modules. In the corresponding selection box, the user can specify a severity (debug, warning, error and fatal in increasing severity) of the event. The user may also choose to search all of the severities.



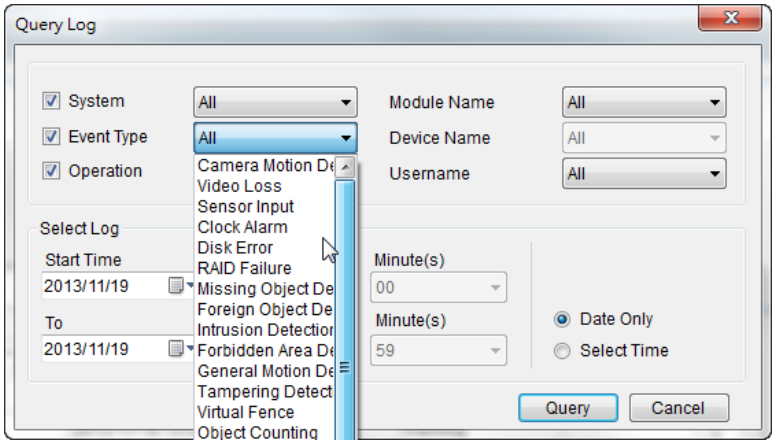
Module Name

The corresponding subfield for *System Type* is *Module Name*. In this selection box, the user can specify a module to search for errors on. The user may also choose to search over all modules by choosing **All**.



Event Type

These include errors that occur with cameras. Events include motion detection, video loss, sensor input, clock alarm, disk error and RAID failure. The user may also choose to search over all these types.

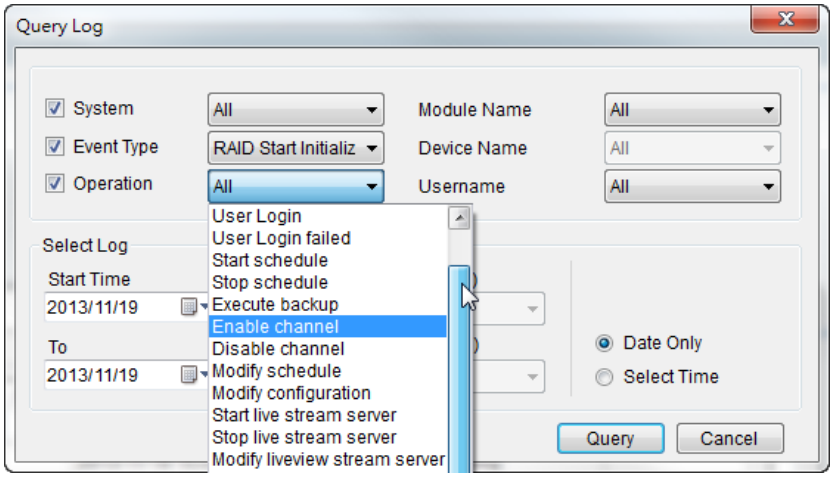


Device Name

This subfield contains a list of all the cameras installed on the system. The events can be further narrowed to focus on a single camera by choosing it, or the search can be done over all cameras by choosing **All**.

Operation Type

These events include the console startup and stop, system usage, and other events that occur during system operation.



User Name

Using the *User Name* subfield a search can be narrowed down to an individual user. This selection list contains all the users configured on the system. All the users can be included by selecting **All.**

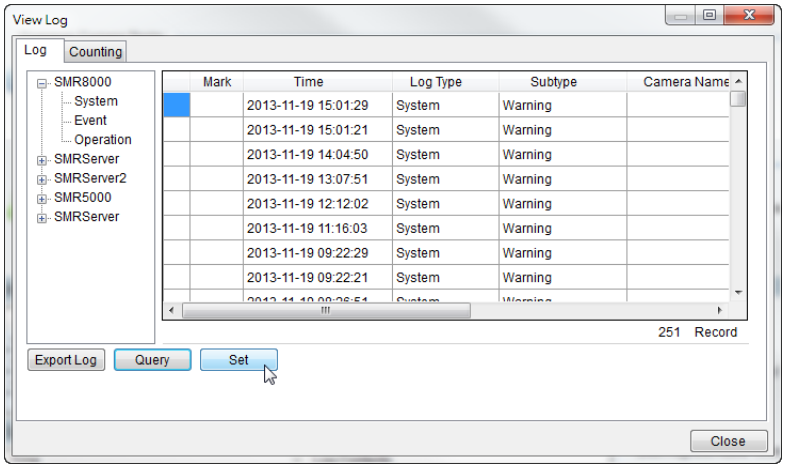
Performing a Search

To perform a search of the log files:

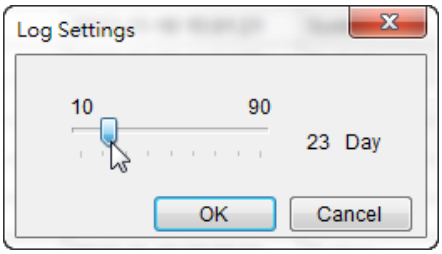
1. If desired, narrow the search by selecting an event type and subfield to search over. More than one event type can be searched.
2. Choose a start date and an end date to search over using the calendar drop-downs.
3. If desired, click **Select time** and select an hour and minute for the start and end times to further narrow the search.
4. Click the **Query** button. The results will show in the main *View Log Screen*. Mousing over individual entries will display the details for that entry at the bottom of the *Log Viewer*.

6.4.3. Event Log Setup

The event log settings can be changed by clicking on the **Set** button located at the bottom of the *View Log* screen.

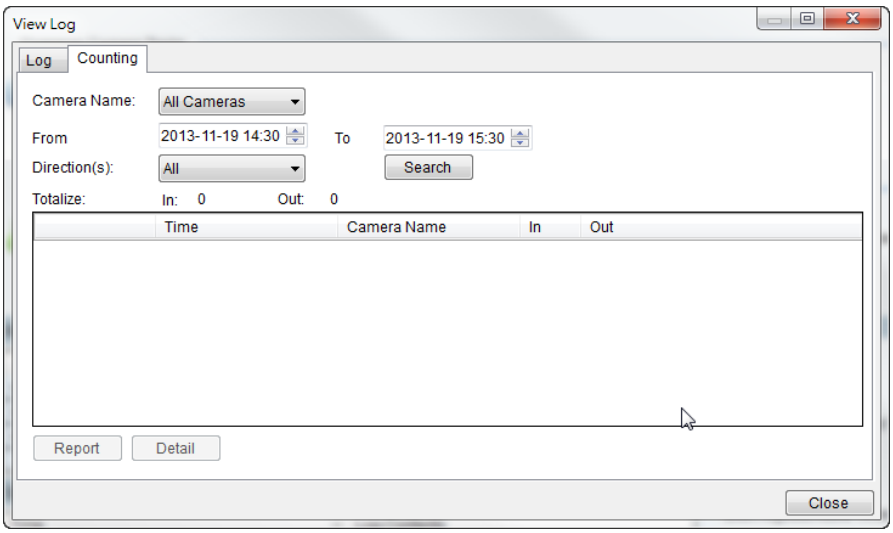


From this screen, the slider can be adjusted set the number of days that the system will store each type of log. Days range from 10 to 90 days.

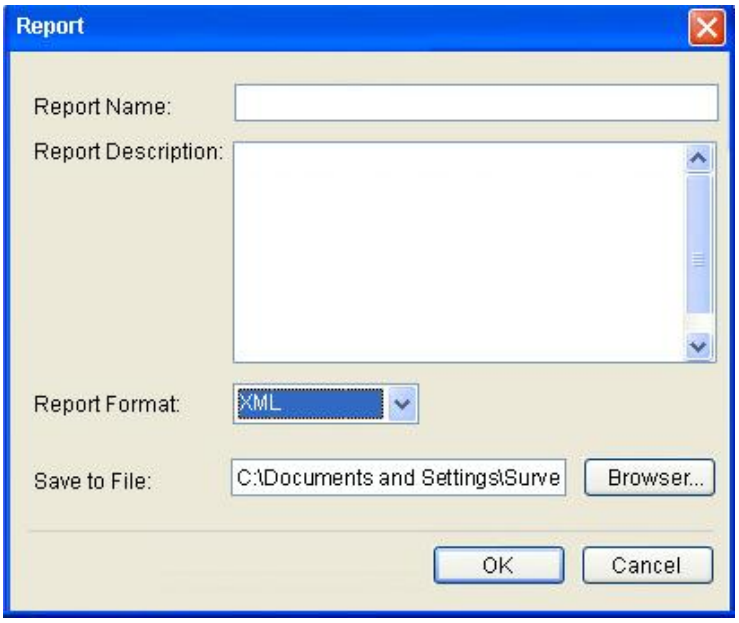


6.4.4. Log for Object Counting

Users can adjust the object counting duration and see the statistical results by choosing the *Counting* tab in the *View Log* Window.



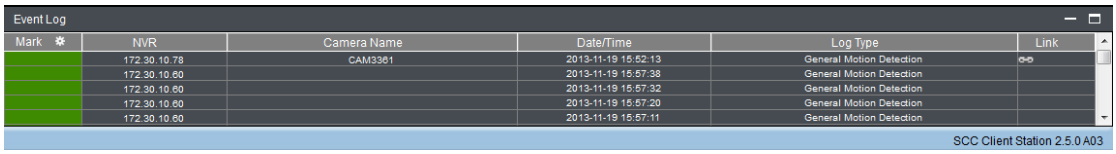
Object counting report can be exported by clicking the Report button:



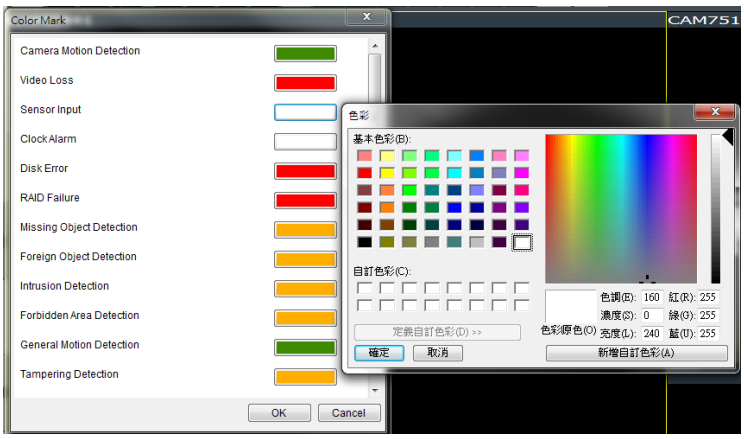
1. Input the report name and report descriptions:
   - **Report name**: Cannot be NULL. MAX: 64 bytes.
   - **Report description:** MAX: 1024 bytes.
2. Select the report format.
3. Specify a directory for file saving.

6.4.5. Event Log View

The event log will also be displayed at the bottom of the Live View screen.



1. **Mark***: double click this item to further define the color bar shown on the Event Log.



2. **NVR**: the IP Address of the NVR
3. **Camera Name**: the camera being alarm-triggered
4. **Date/Time**: when the triggered event was taken place.
5. **Log Type**: alarm type
6. **Link**: clink the link can be directed to the playback to see the triggered moment.

Chapter 7. Search and Playback

In many cases, such as investigations or for reference purposes, it may be useful to be able to replay video streams. The Server has the ability to store video from the IP cameras, as well as playback and export this video information.

7.1. Introduction

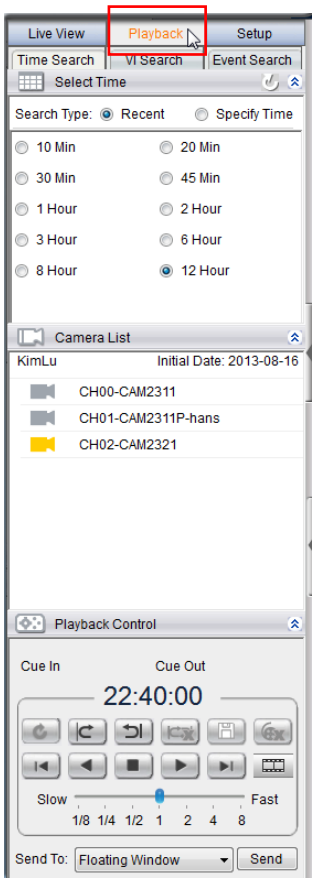
Note: You must be logged **into** a server to access playback functionality.

The SCC has 3 distinct playback functions:

- Time Search – Plays back according to a time period specified by the user.
- VI Search – Applies VI functionalities to a recorded video stream.
- Event Search – Searches the video stream for distinct events.

Note: Event Search is recommended rather than VI Search, since VI Search uses more bandwidth.

These functions may be accessed by clicking on the *Playback* tab located directly above the *Device Browser* window in the live view screen.



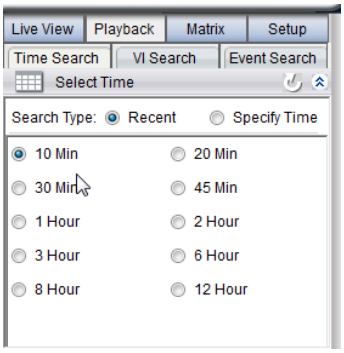
7.2. Date/Time Search

Time based playback can be accessed using the **Time Search** tab at the top of the screen. This search allows you to specify the time of the clip you want to view.

7.2.1. Time Selection

There are two types of time selections that can be made: Recent Time and Specified Time.

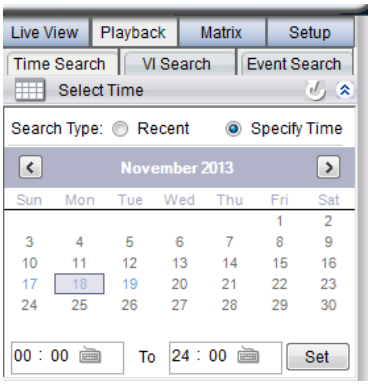
Recent Time



To perform a recent time search, click the **Recent** option in the time selection box. Choose one of the simple time choices to perform playback/search from that time period.

Specified Time

A specified time search can be selected by choosing the **Specify Time** option from the time selection box, and involves defining a time and date for the playback/search. Using the calendar and time boxes, specify a specific period to search/playback.



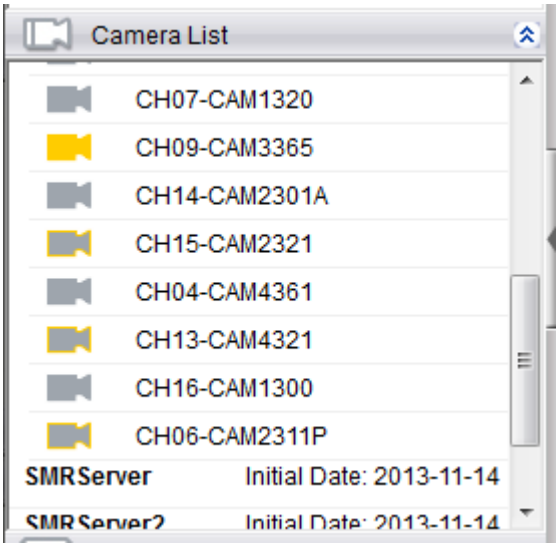
7.2.2. Use of 1x/4x Views

Users have the option of viewing up to 4 recorded video streams at once, or just one stream at a time. Either of these options can be chosen by clicking on corresponding button in the button area above the main view screen. In both cases functionality and operation is the same.

Note: 4x view is not available for SMR series.

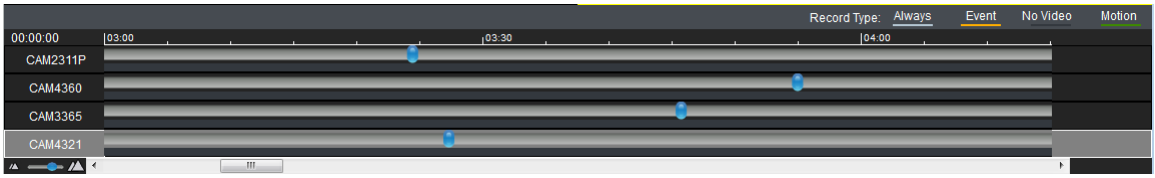
7.2.3. Camera Selection

Once a time period has been selected, the cameras available for each period will be listed in the *Camera List*. These cameras can then be dragged into one the search/playback box(es).



7.2.4. Timeline

After choosing the cameras to view, the timeline for the camera is displayed below the video window.

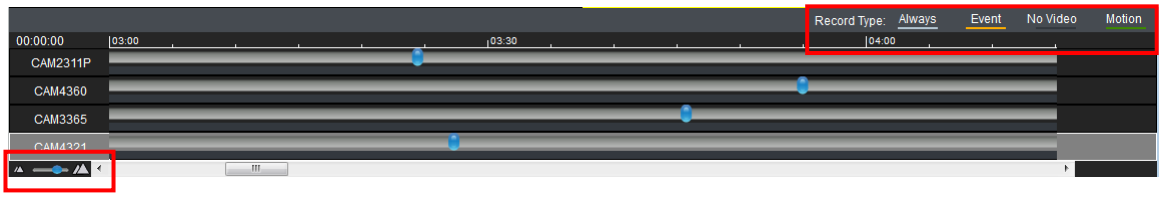


The timeline window displays a graphic representation of the video information available for the camera on the date and timeframe you have chosen in the *Select Date* window. You may choose to reset the timeframe to be displayed by using the dropdown at the top of the timeline.

The timeline will, at most, show a period of a little more than 3 hours. If the timeframe that you desire to view is larger than this, the remaining portion of the timeline can be viewed by using the scrollbar located beneath the timeline.

The amount of time displayed in the timeline can also be adjusted using the slider located next to the scrollbar. Sliding the indicator toward the right will cause a smaller amount of time to be displayed along the length of the timeline. In 4 camera mode, the timelines for the separate feeds will be locked to the same time period.

Once a timeline is loaded, the viewer will be able to see what kind of information is available. The timeline will be divided into 5-minute segments, with each segment colored according to what type of information it contains.



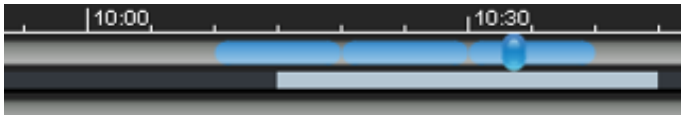
The colors are explained below:

Color	Meaning
Light Grey	The camera was set to Record Always and there is video
Yellow	Video due to an alarm trigger
Dark Grey	There is no video for this segment.

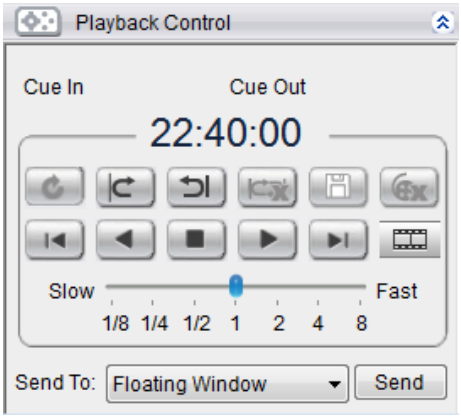
There are also two types of events that will be recorded on the timeline. These events will be displayed as vertical striping on the normal color. If a motion sensor has been triggered during a period of recording, vertical red stripes will appear, and if another type of sensor (pressure, window/door, etc) is triggered, vertical green stripes will appear.

7.2.5. Playback

Once a timeline has been loaded, you may choose the point to begin playback. This is done by clicking the timeline. After selecting the start point you may start playback.



To start playback of a camera's video feed, ensure that the video is selected (the pane, timeline and camera name will be highlighted in yellow). Select feeds by clicking the corresponding pane, timeline, or camera name. Once you have selected a camera, you may use the buttons in the *Playback Control Area* to control the playback. Playback time is denoted above the control buttons.



Note: The system may take a while to buffer the video before playback starts. A status line above the timeline will indicate portions that have been buffered. Jumping to unbuffered points in the video will cause the system to display an error message.

Clicking on a selected portion of the timeline will cause playback to jump to the point that you have clicked on. You must start playback separately for each feed you wish to view.

The following table explains the buttons:

	Starts video playback.
	Reverses video playback.
	Stops video playback.
	Jumps to the next segment.
	Jumps to the previous segment.
	Clears the cue-in and cue-out markers.
	Set Cue-In marker for clip start
	Set Cue-Out marker for clip end
	Loop, continuous playback within Cue-In & Cue-Out
	Saves video clips/Exports selected clips.
	Deletes selected clips
	Real time mode
	Frame by frame mode
	Just key frame mode

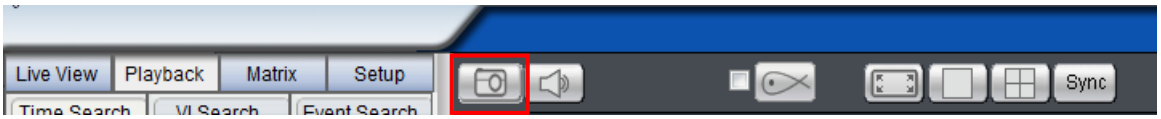
Synchronized Playback

At most 4-channel concurrent and synchronized playback can be displayed by clicking the **Sync** button in the button area.

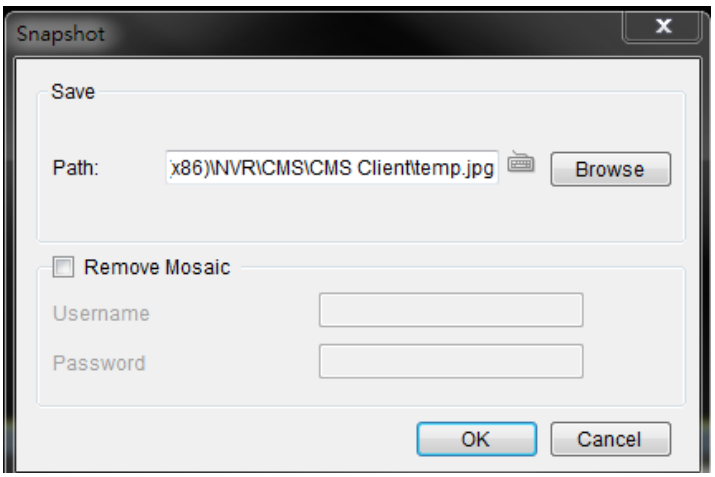
Note: 4-channel synchronized playback is not available for SMR series.

Capturing Snapshot

1. Click the **Capture** button located in the button area.



2. In the **Path** field enter a file path and filename for the screenshot. Alternately, you may also click **Browse** and select a file path.
3. **(Optional)** You may click **Remove Mosaic** and enter a valid **Username** and **Password** to remove any privacy-mask mosaicing.

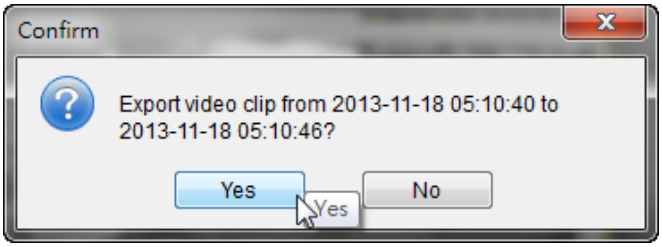


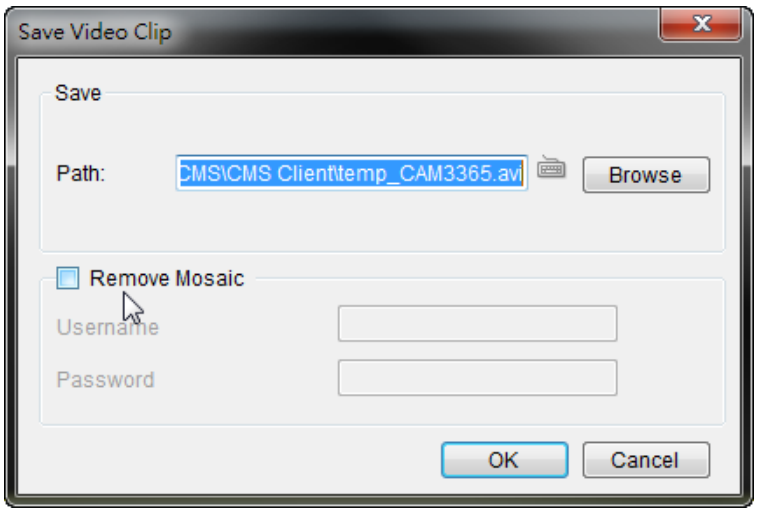
4. Click **OK** to save the screenshot.

Capturing Video Clip

1. Make sure that the video clip is playing.
2. When the beginning of the segment to be captured is reached, click the **Cue In** button.

3. When the end of the segment to be captured is reached, click the **Cue Out** button.
4. Click the **Save Video Clip** button beside the **Cue In** and **Cue Out** buttons. A system popup will open prompting for a filename and location for the video clip.

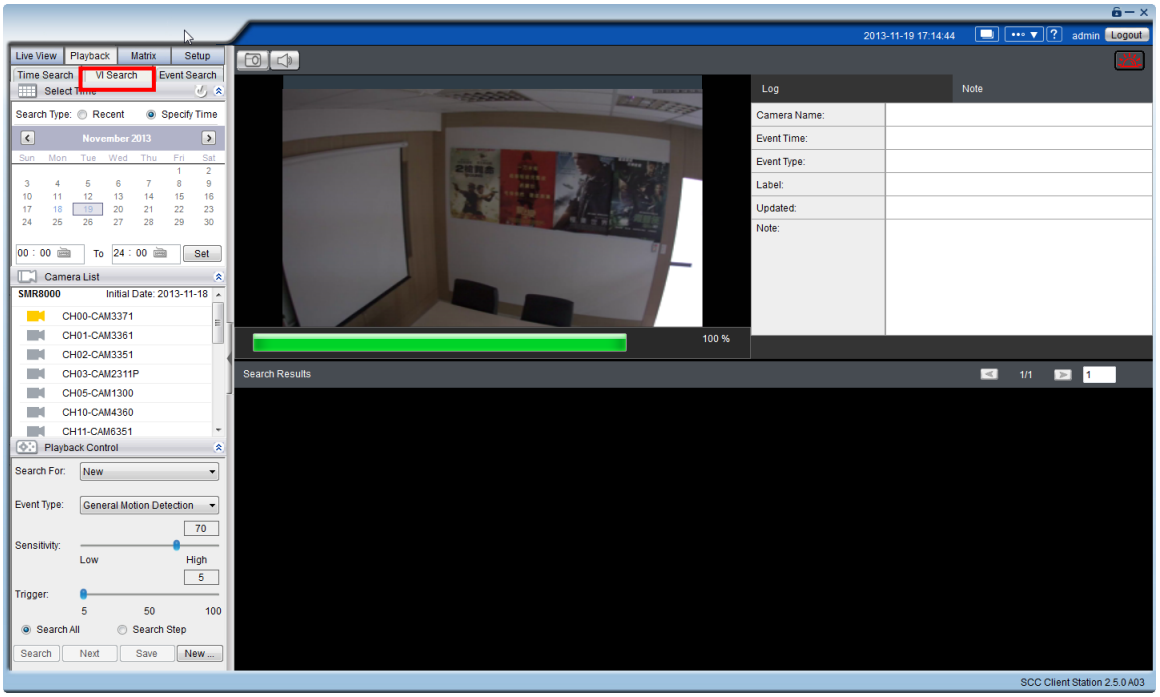




5. **(Optional)** Change the filename and file path. If you do not change the file details, the default save location for the video clip will be your installation path.
6. **(Optional)** You may click **Remove Mosaic** and enter a valid **Username** and **Password** to remove any privacy-mask mosaicing.

7.3. VI Search

A VI search involves applying VI to existing recorded video in order to locate a specific event or action. To access the VI search, click the *VI Search* tab in the *Playback* context.



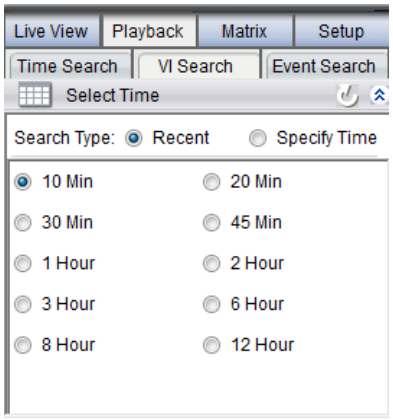
7.3.1. Creating a VI Search

Time Selection

There are two types of time selections that can be made for each playback: Recent Time and Specified Time.

Recent Time

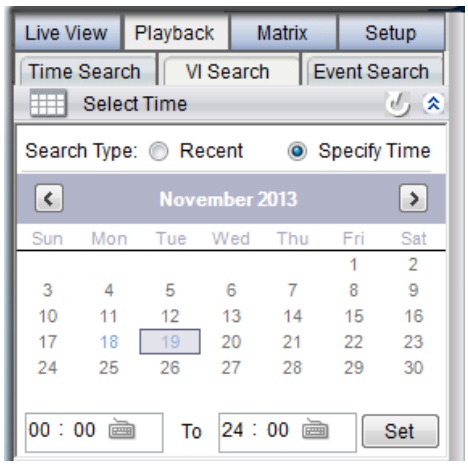
To perform a recent time search, click the **Recent** option in the time selection box. Choose one of the simple time choices to perform playback/search from that time period.



Specified Time

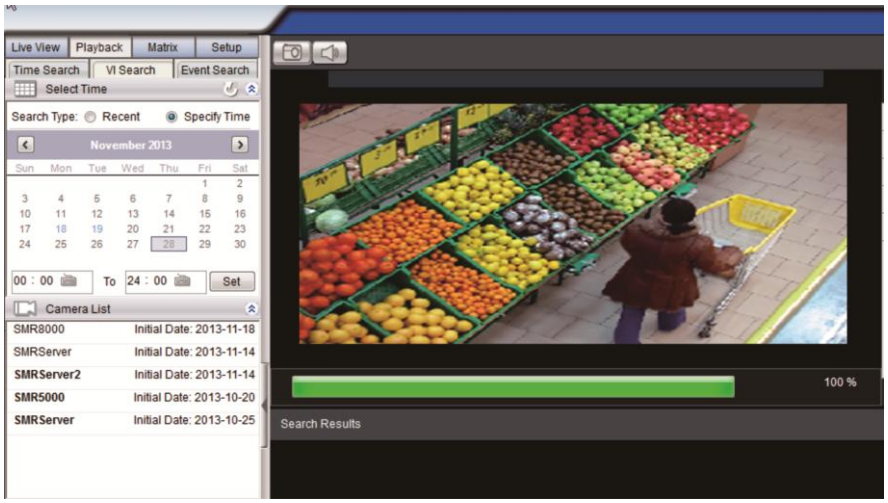
A specified time search can be selected by choosing the **Specify Time** option from the time selection box, and involves defining a time and date for the playback/search.

Using the calendar select a date for search/playback. Once a date is selected, clicking on the boxes will allow you to specify a specific period to search/playback in 10 minute increments.



Camera Selection

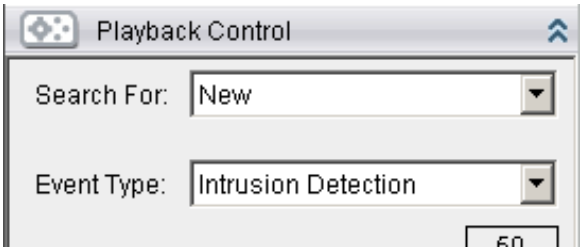
Once the search time range has been specified, a list of cameras with video recorded during the period specified will appear in the *Camera List*.



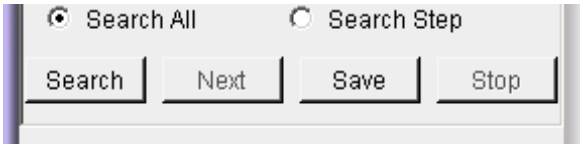
Select a camera to perform the VI search on by clicking its entry. This will display an initial thumbnail of the camera output.

Setting New Search Criteria

To create a New VI search:



1. **New** in the playback control.
2. Follow directions in the following sections to set up the VI search.
3. Once the VI search is set up select either:
   - **Search All** - Finds all events within the search range that trigger the VI set up.



   - **Search Step** – Finds the first event that triggers the VI, then stops. The next event can be found by repeating the same search.
4. Click **Search** to begin the VI Search.

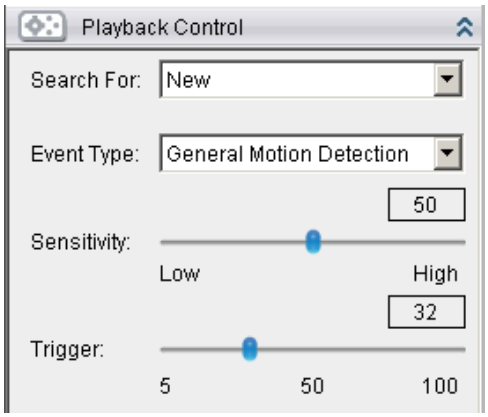
General Motion Detection

General motion detection involves detecting motion in specified areas. To set up General Motion Detection:

1. Select General Motion Detection from the Event Type dropdown.
2. **New** button to create a detection window. Up to 3 detection windows can be set for each camera. The current window will be highlighted with a red border.

3. Click and drag the white dots along window border of a window to resize or reshape the window. Click the interior of windows and hold to drag to reposition them. Move and resize windows until the area of detection is covered.

4. Adjust the sliders in the *Playback Control* section. (Settings will be applied to all existing windows)

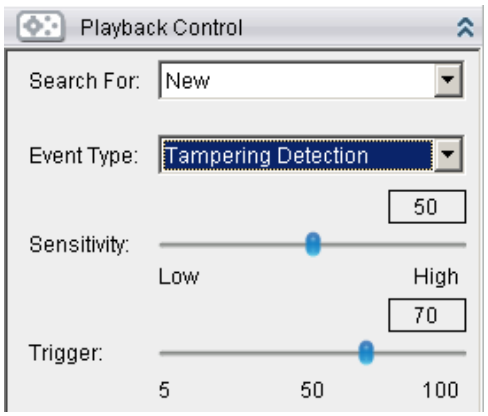


- **Sensitivity** - Adjusts window sensitivity from 0 (low) to 100 (high).
- **Trigger** - Adjusts the amount of change allowed before and event is triggered.

Tampering Detection

Tampering detection involves using the software to determine when the camera has been improperly moved or redirected. To configure:

1. Select Tampering Detection from the Event Type dropdown.
2. Adjust the sliders:
   - **Sensitivity** - Adjusts window sensitivity from 0 (low) to 100 (high).
   - **Trigger** - Adjusts the amount of change allowed before an event is triggered.



Intrusion Detection

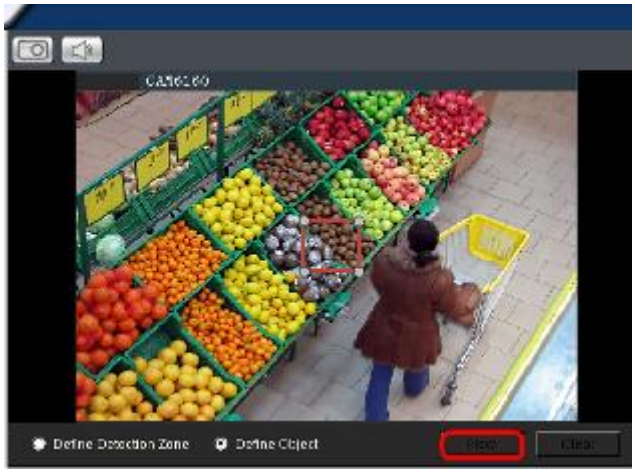
Intrusion detection involves using the software to analyze the video feed and detect intrusion in specified areas. To configure:

1. Select Intrusion Detection from the Event Type dropdown.

2. Select **Define Detection Zone** and click the **New** button to create a new window. Up to 3 detection windows can be set for each camera. The current window will be highlighted with a red border.

3. Click and drag the white dots along window border of a window to resize or reshape the window. Click the interior of windows and hold to drag to reposition them. Move and resize windows until the area of to be secured is covered.

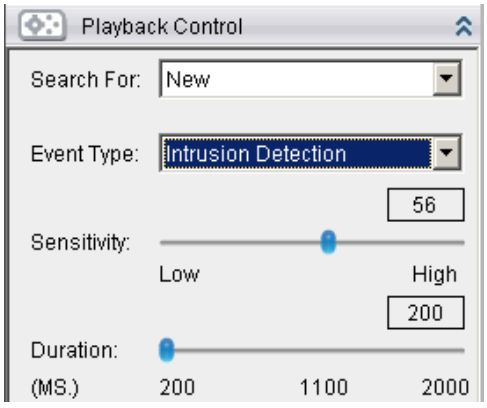
4. Select **Define Object** and click the **New** button to create an object box.



5. Click and drag the white dots along the window border to resize it and define the minimum size of objects that will be detected.

6. Adjust the sliders in the *Playback Control* section. (Settings will be applied to all existing windows)

- **Sensitivity** - Adjusts window sensitivity from 0 (low) to 100 (high).
- **Duration (Msec) -** Adjusts how much time between each check of the window for intrusions.



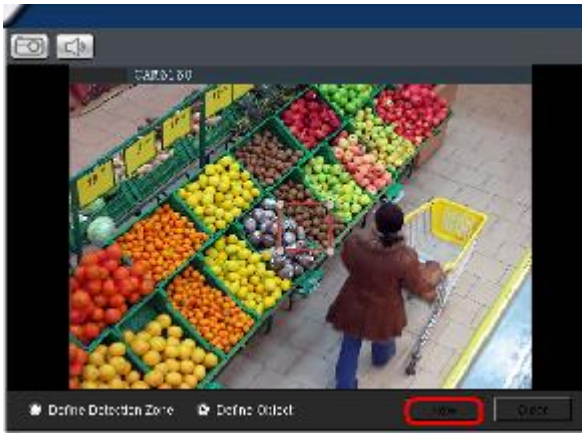
Missing Object Detection

Missing object detection involves using the software to analyze the video feed and detect missing objects larger than a certain size. To configure:

1. Select Missing Object Detection from the Event Type dropdown.
2. Select **Define Detection Zone** and click the **New** button to create a new window. Up to 3 detection windows can be set for each camera. The current window will be highlighted with a red border.

3. Click and drag the white dots along window border of a window to resize or reshape the window. Click the interior of windows and hold to drag to reposition them. Move and resize windows until the area to be secured is covered.

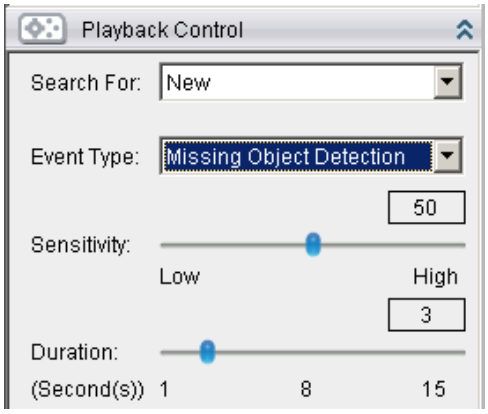
4. Select **Define Object** and click the **New** button to create an object box.



2. Click and drag the white dots along the window border to resize it and define the minimum size of the object(s) that will be secured.

3. Adjust the sliders in the *Playback Control* section. (Settings will be applied to all existing windows)

- **Sensitivity** - Adjusts window sensitivity from 0 (low) to 100 (high).
- **Duration (Sec) -** Adjusts how much time an object is missing before an event is triggered.



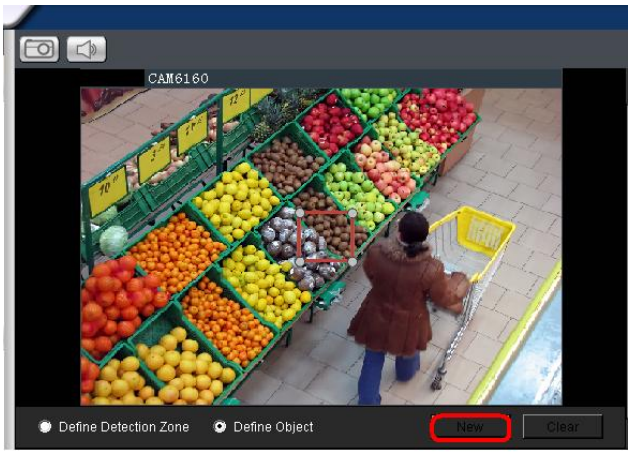
Foreign Object Detection

Foreign object detection involves using the software to analyze a video feed and detect objects that do not belong. To configure:

1. Select Foreign Object Detection from the Event Type dropdown.
2. Select **Define Detection Zone** and click the **New** button to create a new window. Up to 3 detection windows can be set for each camera. The current window will be highlighted with a red border.

3. Click and drag the white dots along window border of a window to resize or reshape the window. Click the interior of windows and hold to drag to reposition them. Move and resize windows until the area of detection is covered.

4. Select **Define Object** and click the **New** button to create an object box.

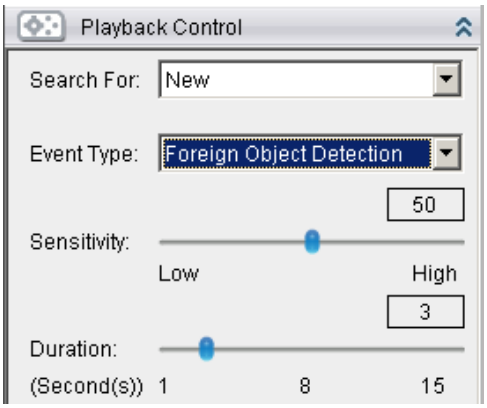


5. Click and drag the white dots along the window border to resize it and define the minimum size of foreign objects that will be detected.

6. Adjust the sliders in the *Playback Control* section. (Settings will be applied to all existing windows)

- **Sensitivity** – Adjusts window sensitivity from 0 (low) to 100 (high).

- **Duration (Sec)** - Adjusts the amount of time before an object triggers an event.



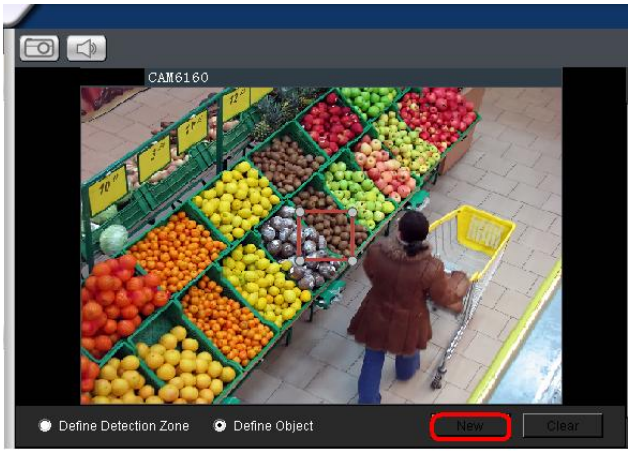
Forbidden Area Detection

Forbidden area detection involves using the software to analyze the video feed and immediately detect any object in specified areas. To configure:

1. Select Forbidden Area Detection from the Event Type dropdown.
2. Select **Define Detection Zone** and click the **New** button to create a new window. Up to 3 detection windows can be set for each camera. The current window will be highlighted with a red border.

3. Click and drag the white dots along window border of a window to resize or reshape the window. Click the interior of windows and hold to drag to reposition them. Move and resize windows until the forbidden area is covered.

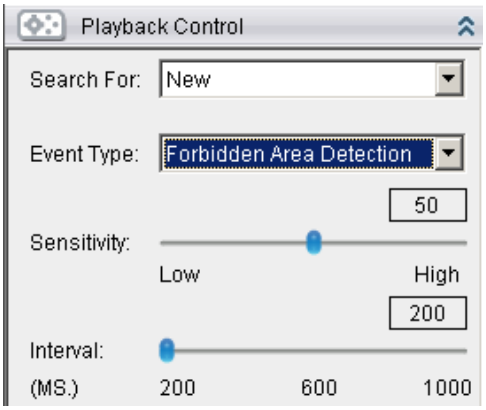
4. Select **Define Object** and click the **New** button to create an object box.



5. Click and drag the white dots along the window border to resize it and define the minimum size of objects that will be detected.

6. Adjust the sliders in the *Playback Control* section. (Settings will be applied to all existing windows)

- **Sensitivity** - Adjusts window sensitivity from 0 (low) to 100 (high).
- **Interval** - Adjusts how much time between each check of the forbidden area.



Virtual Fence

Virtual fence involves using the software to create a fence-crossing detection of the demanding object. To configure:

1. Select Virtual Fence from the Event Type dropdown.
2. Select **Define Detection Zone** and click the **New** button to create a new window. Up to 3 detection windows can be set for each camera. The current window will be highlighted with a one/two-way arrow (blue means "in", green means "out").

3. Click and drag the white arrows along the window border around the one/two-way arrow to resize the space between the fences/adjust the length of the fences.
4. Turn the window border with the orange arrow to change the directions of the fences.
5. Select **Define Object** and click the **New** button to create an object box.
6. Click and drag the white dots along the window border to resize it and define the minimum size of objects that will be detected.
7. Adjust the sliders in the *Playback Control* section. (Settings will be applied to all existing windows)
   - **Sensitivity** - Adjusts window sensitivity from 0 (low) to 100 (high).
   - **Duration (Sec)** - Adjusts how much time between each check for the fence-crossing.

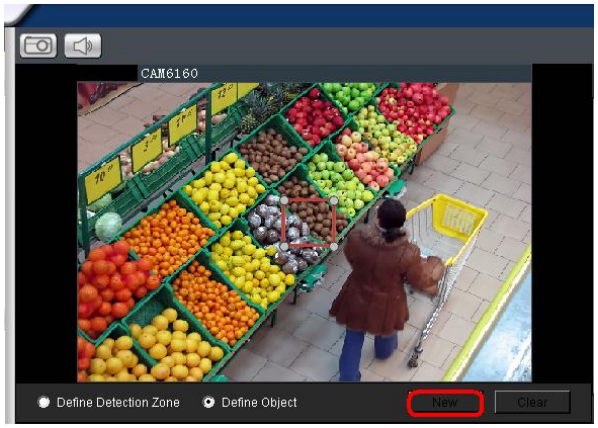
Going Out Detection

Going Out detection involves using the software to analyze the video feed and immediately detect any object in specified areas. To configure:

1. Select Going Out Detection from the Event Type dropdown.
2. Select **Define Detection Zone** and click the **New** button to create a new window. Only 1 detection window can be set for each camera. The current window will be highlighted with a red border.

3. Click and drag the white dots along window border of a window to resize or reshape the window. Click the interior of windows and hold to drag to reposition them. Move and resize windows until the Going Out boundary is done.

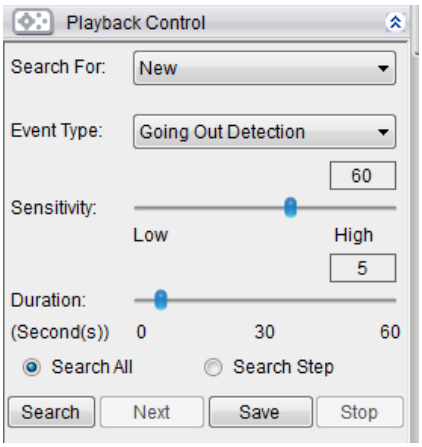
4. Select **Define Object** and click the **New** button to create an object box.



5. Click and drag the white dots along the window border to resize it and define the minimum size of objects that will be detected.

6. Adjust the sliders in the *Playback Control* section. (Settings will be applied to all existing windows)

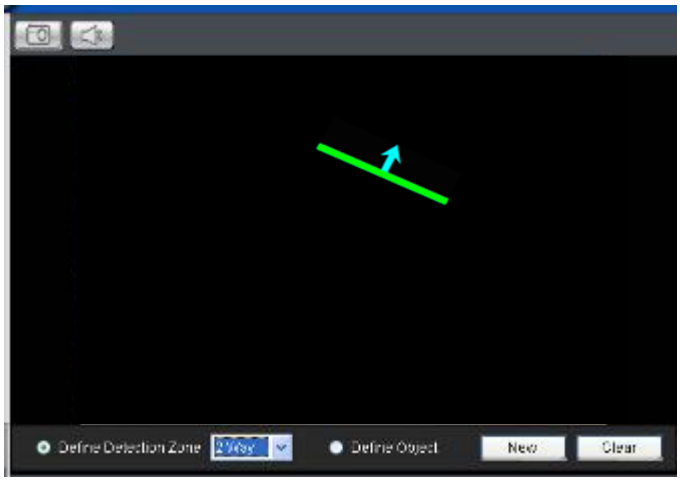
- **Sensitivity** – Adjusts window sensitivity from 0 (low) to 100 (high).
- **Interval** - Adjusts how much time between each check of the forbidden area.



Tailgating Detection

Tailgating Detection involves using the software to create a fence-crossing detection of the demanding object. To configure:

1. Select Tailgating Detection from the Event Type dropdown.
2. Select **Define Detection Zone** and click the **New** button to create a new window. Only 1 detection window can be set for each camera.



3. Click and drag the arrow to adjust the position and direction.
4. Select **Define Object** and click the **New** button to create an object box.
5. Click and drag the white dots along the window border to resize it and define the minimum size of objects that will be detected.
6. Adjust the sliders in the *Playback Control* section. (Settings will be applied to all existing windows)
   - **Sensitivity** - Adjusts window sensitivity from 0 (low) to 100 (high).
   - **Duration (Sec)** - Adjusts how much time between each check for the fence-crossing.

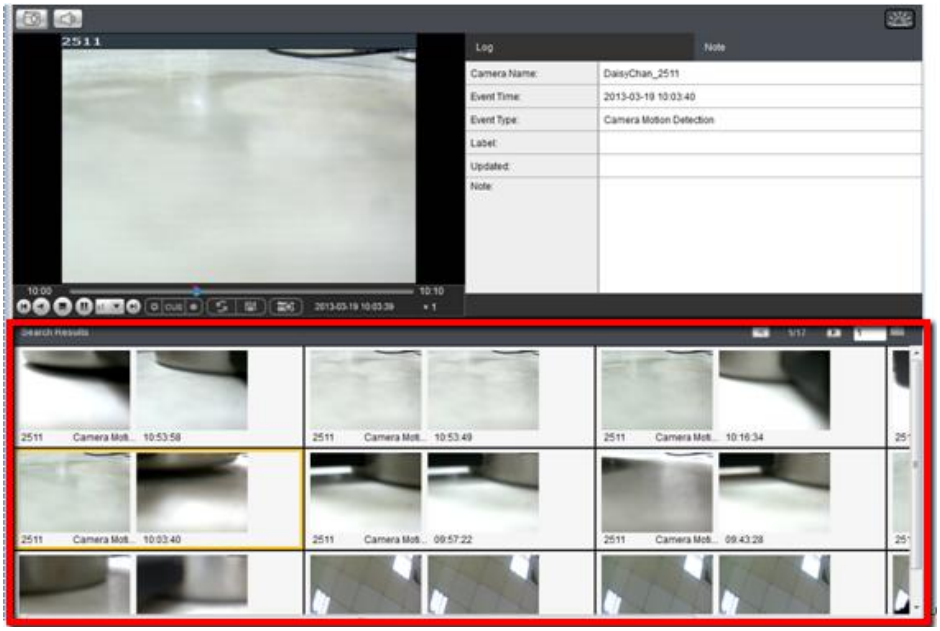
7.3.2. Saving/Retrieving a VI Search

Once the VI search is setup, you may save it by clicking the **Save** button. The system will prompt you for a name. Saved VI searches can also be retrieved using the **Search for** dropdown, or by clicking the **Next** button.

7.3.3. Using the Search Results

Selecting the Result

Search result thumbnail(s) will be displayed in the results box.



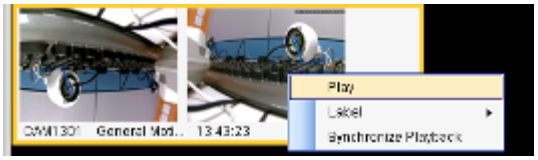
Clicking the thumbnail will select the detection instance. The following information fields are available for each instance:

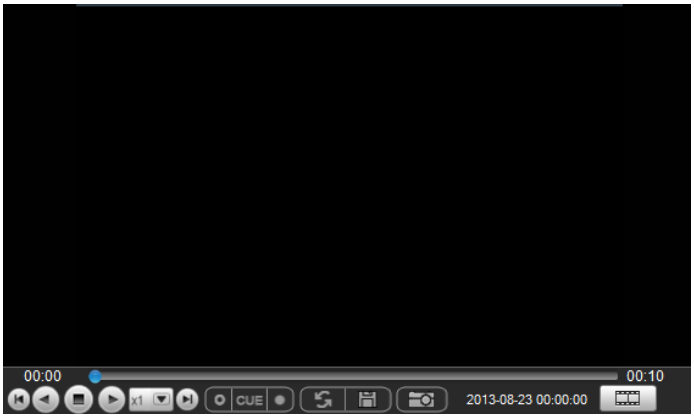
Log	Note
Camera Name:	DAISYCHAN_CAM1301
Event Time:	2012-02-20 13:43:23
Event Type:	General Motion Detection
Label:	
Updated:	
Note:	

- **Camera Name** – The camera used to capture the video.
- **Event Time** – The time the event occurred.
- **Event Type** – The type of VI detection that the event triggered.
- **Label** – A user-defined label (optional).
- **Updated** - The last time the event was updated.
- **Note** - A simple comment or note for the clip.

Result Playback

Once a result is selected by clicking on it, playback can be started by double clicking on the thumbnail. Alternatively, you may right-click the thumbnail and click **Play**. A ten minute clip containing the event will begin playing, with the start time synchronized with the start of the event.





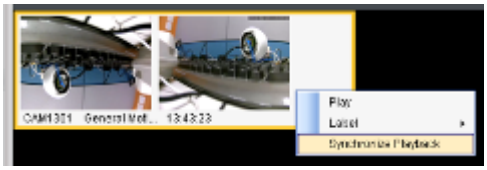
The following functions are available for playback:

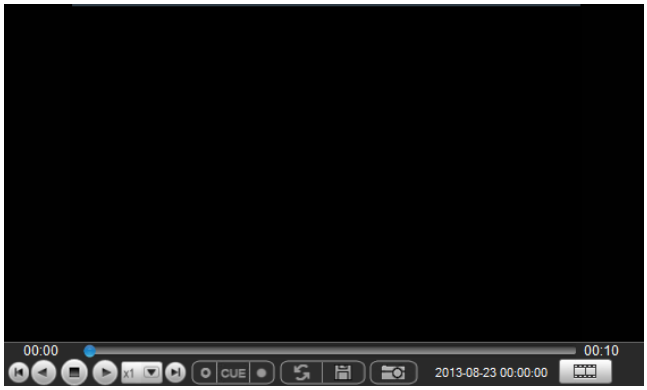
	Starts video playback.
	Reverses video playback.
	Stops video playback.
	Jumps to the next segment.
	Jumps to the previous segment.
	Clears the cue-in and cue-out markers.
	Set Cue-In marker for clip start
	Set Cue-Out marker for clip end

	Loop, continuous playback within Cue-In & Cue-Out
	Enable / Disenable loop. Loop to continuous playback within Cue-In & Cue-Out.
	Saves video clips/Exports selected clips.
	Snapshot
	Real time mode
	Frame by frame mode
	Just key frame mode

Playback Synchronization

Search results can be sent to the time-based playback window for comparison with other video streams using the **Synchronize Playback** function. This action will send the 10 minute segment containing the detected event to the time-based playback window.

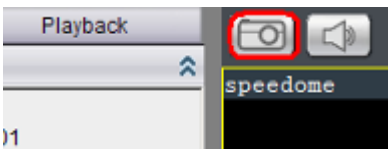




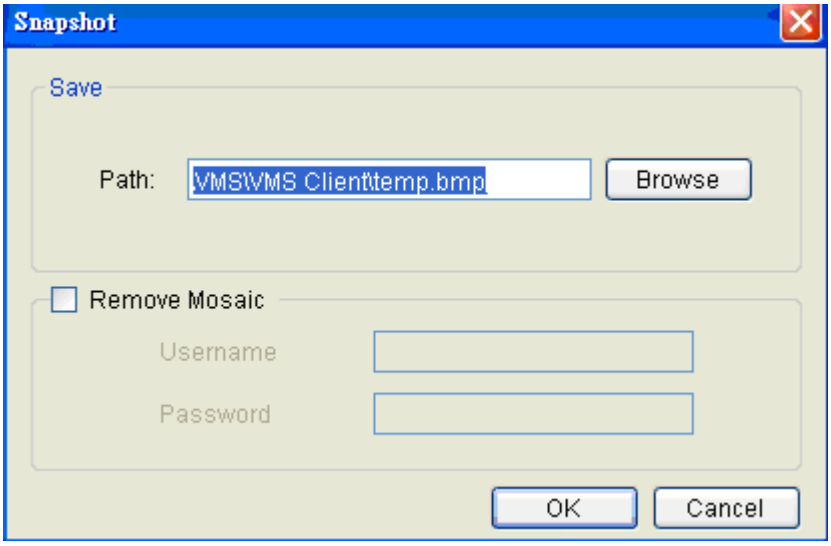
Capturing Snapshot

To capture a screenshot:

1. Click the **Capture** button located in the button area.



2. In the **Path** field enter a file path and filename for the screenshot. Alternately, you may also click **Browse** and select a file path.



3. **(Optional)** You may click **Remove Mosaic** and enter a valid **Username** and **Password** to remove any privacy-mask mosaicing.

4. Click **OK** to save the screenshot.

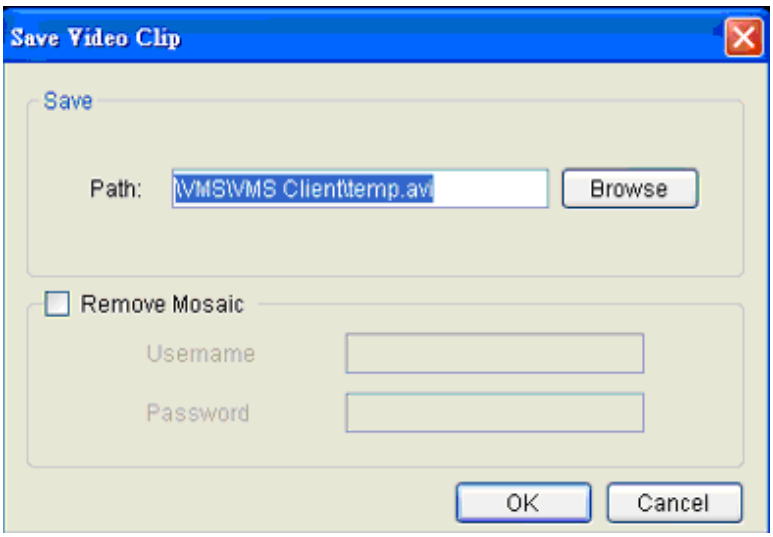
Capturing Video Clip

To capture a video segment:

1. Click the **Cue In** button, and place the marker at the start of the segment to be captured.

2. Click the **Cue Out** button, and place the marker at the end of the segment to be captured.

3. Click the **Save Video Clip** button located in the control area beside the **Cue In** and **Cue Out** buttons. A system popup will open prompting for a filename and location for the video clip.



4. **(Optional)** Change the filename and file path. If you do not change the file details, the default save location for the video clip will be your installation path.

5. **(Optional)** You may click **Remove Mosaic** and enter a valid **Username** and **Password** to remove any privacy-mask mosaicing.

Logging and Noting

Clicking the **Note** tab beside the log entry will let you tag and note the search result for future references.

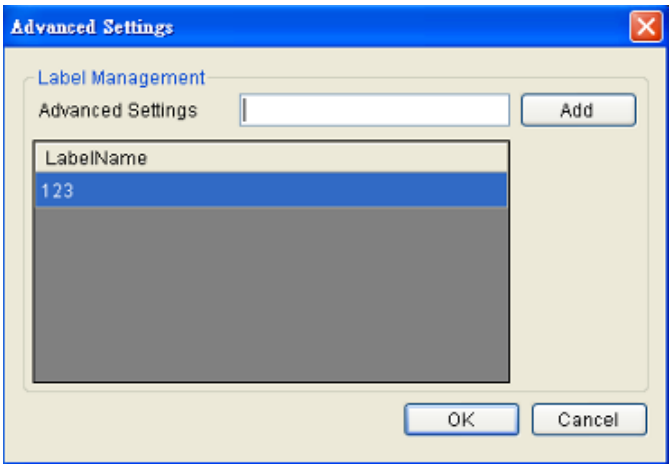
You may choose one of the following:

- **Label** - Select one of the defined labels.
- **Note** - A short description for the video clip.

Label Setup

Clicking **Advanced** from the note context will bring up the label setup menu.

To add a label:

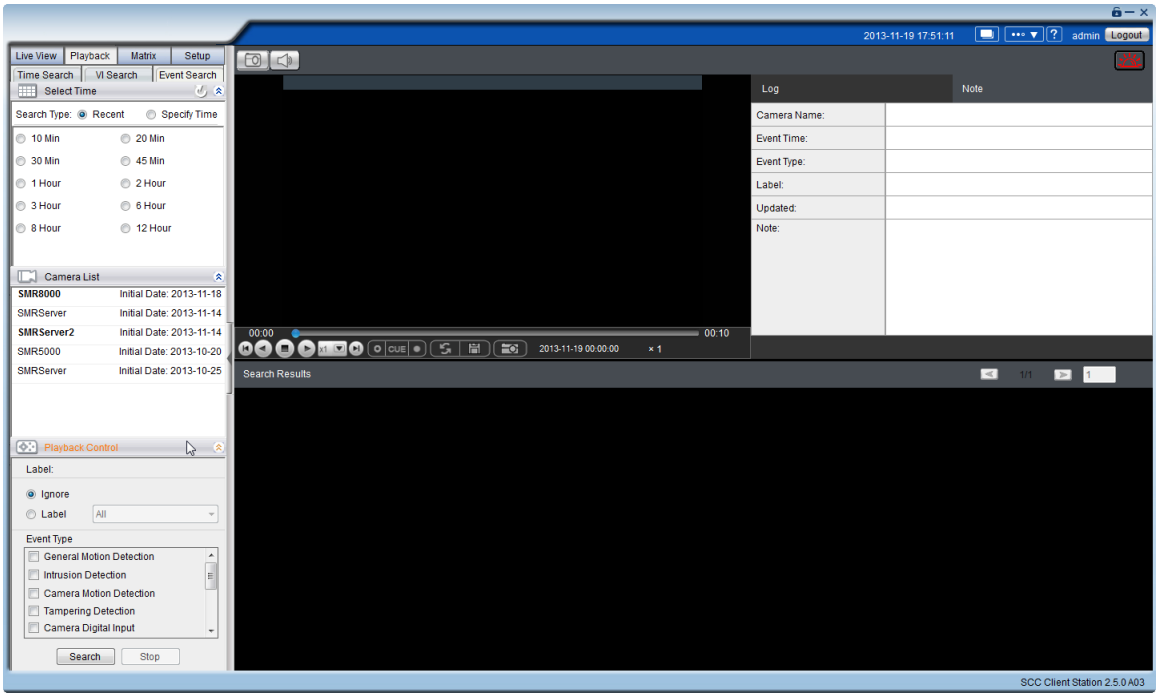


1. Enter a name in the Advanced Settings field.

2. Click **Add**. The new label will appear in the LabelName table. Future clips may be tagged with this label.

7.4. Event Search

An event search involves searching for multiple tagged events over one more cameras. To access Event search, click the **Event Search** tab in the *Playback* context.



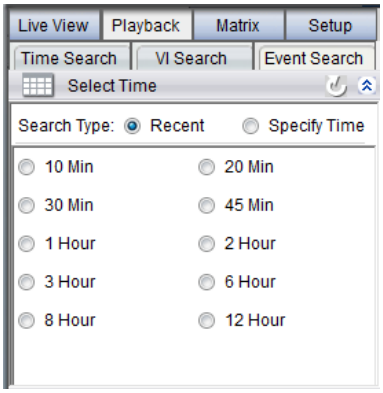
7.4.1. Creating an Event Search

Time Selection

There are two types of time selections that can be made: Recent Time and Specified Time.

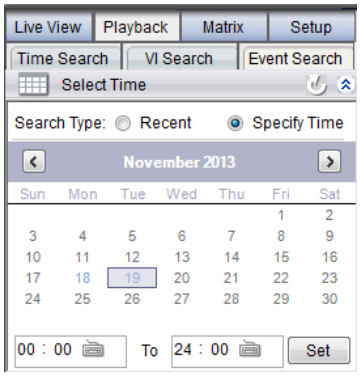
Recent Time

To perform a recent time search, click the **Recent** option in the time selection box. Choose one of the simple time choices to perform playback/search from that time period.



Specified Time

A specified time search can be selected by choosing the **Specify Time** option from the time selection box, and involves defining a time and date for the playback/search.



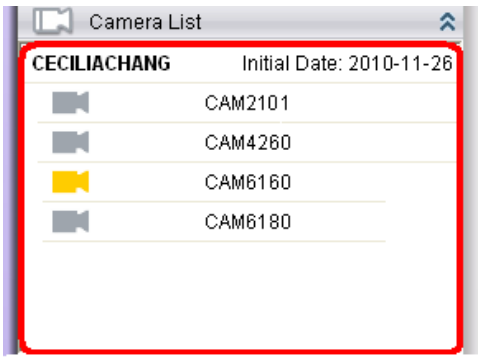
Using the calendar select a date for search/playback. For an event search, multiple dates can be selected by clicking on the calendar and dragging the cursor to select multiple dates. Multiple areas can be selected by pressing the **control** key and selecting additional dates.

Once a date or dates are selected, clicking on the boxes will allow you to specify a specific period to search/playback in 10 minute increments.

Camera Selection

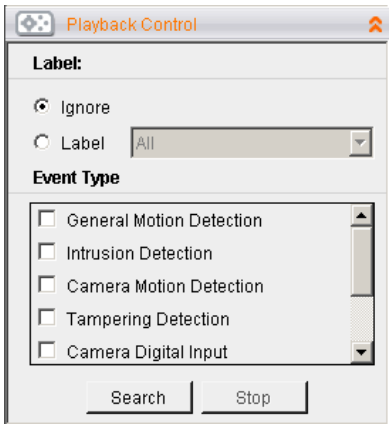
Once the search time range has been specified, a list of cameras with video recorded during the period specified will appear in the *Camera List*.

Select a camera to perform the event search on by clicking its entry. Multiple cameras can be selected for the search.



Setting Event Search Criteria

1. Choose an **Event Type** and/or a **Label** to search for**.** Selecting **Ignore** will search for all labels.

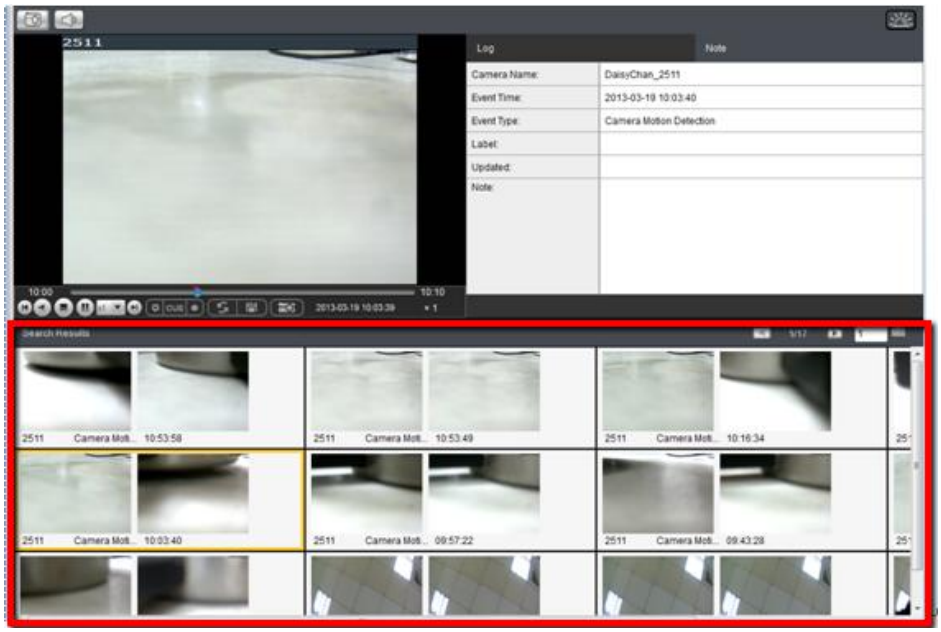


2. Click **Search** to begin the search. Results will display in the *Search Results* panel.

7.4.2. Using the Search Results

Selecting the Result

Search result thumbnail(s) will be displayed in the results box.



Clicking the thumbnail will select the detection instance.

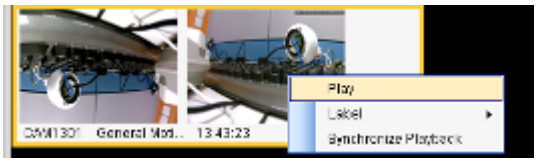
The following information fields are available for each instance:

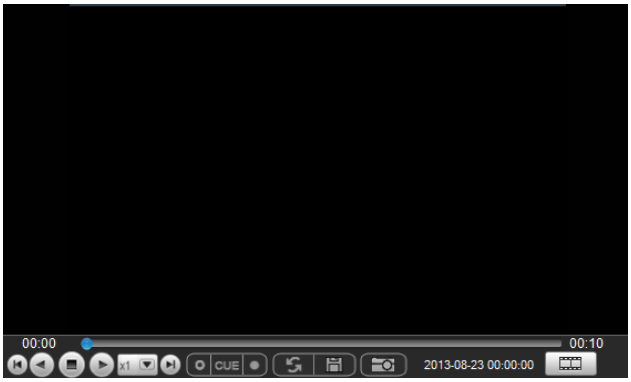
Log	Note
Camera Name:	DAISYCHAN_CAM1301
Event Time:	2012-02-20 13:43:23
Event Type:	General Motion Detection
Label:	
Updated:	
Note:	

- **Camera Name** – The camera used to capture the video.
- **Event Time** – The time the event occurred.
- **Event Type** – The type of VI detection (if any) that the event triggered (optional).
- **Label** – A user-defined label (optional).
- **Updated -** The last time the event was updated.
- **Note -** A simple comment or note for the clip.

Result Playback

Once a result is selected by clicking on it, playback can be started by double clicking on the thumbnail. Alternatively, you may right-click the thumbnail and click **Play**. A ten minute clip containing the event will begin playing, with the start time synchronized with the start of the event.





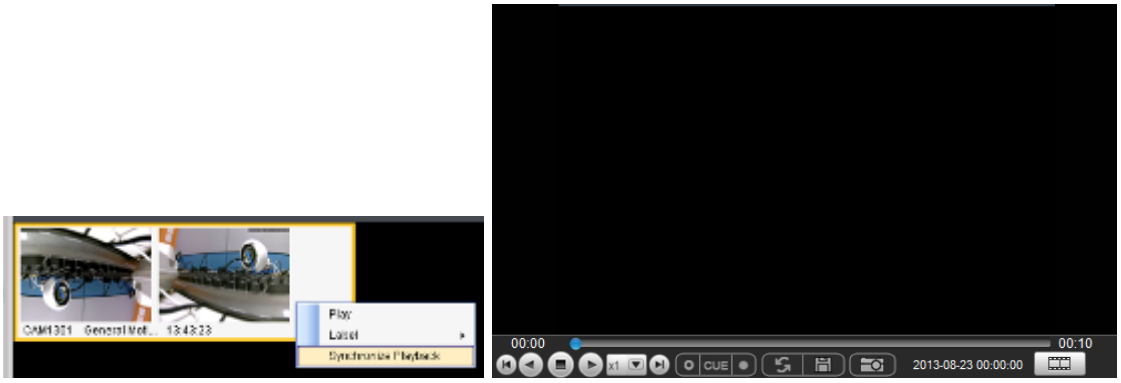
The following functions are available for playback:

	Starts video playback.
	Reverses video playback.
	Stops video playback.
	Jumps to the next segment.
	Jumps to the previous segment.
CUE	Clears the cue-in and cue-out markers.
	Set Cue-In marker for clip start
	Set Cue-Out marker for clip end
	Loop, continuous playback within Cue-In & Cue-Out
	Enable / Disenable loop. Loop to continuous playback within Cue-In & Cue-Out.
	Saves video clips/Exports selected clips.
	Snapshot
	Real time mode

	Frame by frame mode
	Just key frame mode

Playback Synchronization

Search results can be sent to the time-based playback window for comparison with other video streams using the **Synchronize Playback** function. This action will send the 10 minute segment containing the detected event to the time-based playback window.

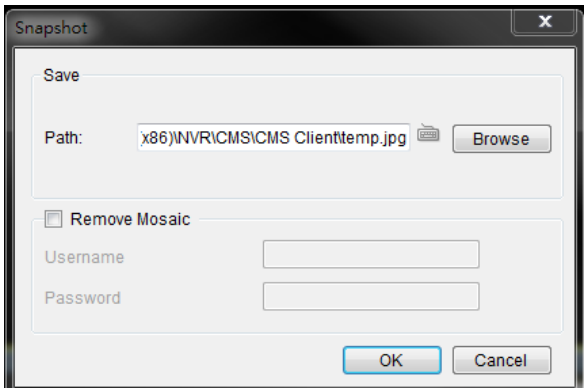


Capturing Snapshot

To capture a screenshot:

1. Click the **Capture** button located in the button area.

2. In the **Path** field enter a file path and filename for the screenshot. Alternately, you may also click **Browse** and select a file path.



3. **(Optional)** You may click **Remove Mosaic** and enter a valid **Username** and **Password** to remove any privacy-mask mosaicing.

4. Click **OK** to save the screenshot.

Logging and Noting

Clicking the **Note** tab beside the log entry will let you tag and note the search result for future references.

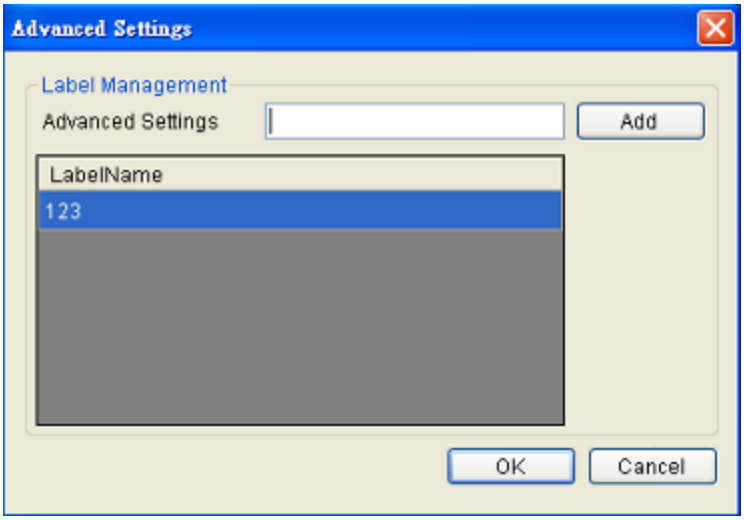
You may choose one of the following:

1. **Label** - Select one of the defined labels.

2. **Note** - A short description for the video clip.

Label Setup

Clicking **Advanced** from the note context will bring up the label setup menu.



To add a label:

1. Enter a name in the Advanced Settings field.

2. Click **Add**. The new label will appear in the LabelName table. Future clips may be tagged with this label.

Chapter 8. Remote Web Client and SPhone Client for Simple Use (Optional)

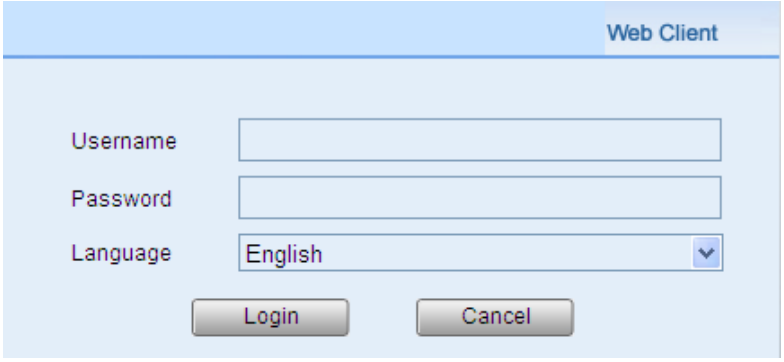
For remote users, there are 3 methods for viewing.

1. Remote Client: install Remote Client on remote PCs for live view and playback.
2. Web Client: use the browser IE (Internet Explorer) and input the IP address of the camera for live view and playback.
3. Mobile Client: install the **Sphone Client** app on iOS or Android mobile devices for basic live viewing.

8.1. Starting the Web Client

Launch Microsoft Internet Explorer 7.0 (or above) and enter your **SCC Server IP address + "/webclient"** in your web browser's URL location, e.g. http://172.18.6.9/webclient to download the Web Client application.

Note: Please check the web server settings in the SCC Console first.



- **Username** – The username for the domain. **Default username is *admin*.**
- **Password** – The password for the domain. **Default password is *admin*.**
- **Language** –Options for the interface languages.

Click **Login** after the username and password are entered.

After logging in, the live view page will be displayed on the web browser.

8.1.1. Checking the Software Version

Users can see the software version at the lower left corner of the window after logging in.

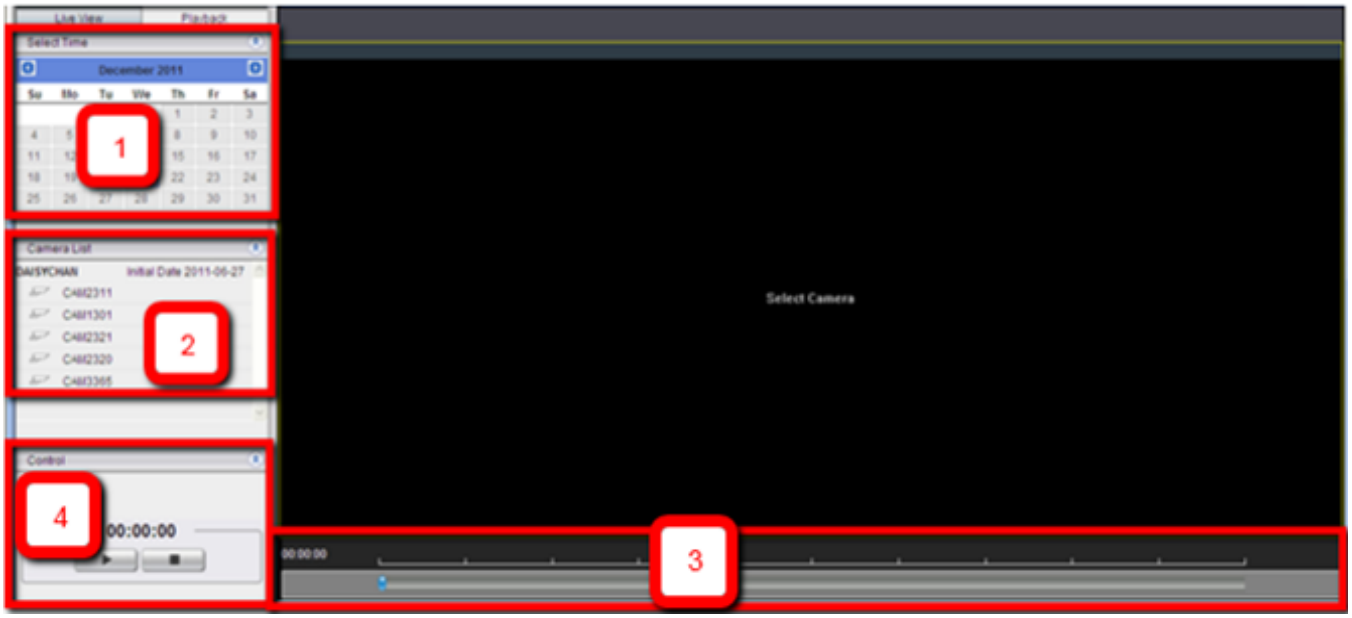
8.1.2. Use of 1x/4x views

Users have the option of viewing up to 4 recorded video streams at once, or just one stream at a time. Either of these options can be chosen by clicking on corresponding button in the button area above the main view screen. In both cases functionality and operation is the same.

8.1.3. PTZ Control

Cameras equipped with Pan-Tilt-Zoom functionality can be controlled directly within the Web Client. These controls can be found in the *PTZ Control* window within the live view screen.

8.1.4. Playback Settings



Users can select the (1) time and (2) camera, and then use the (3) time line and (4) playback control panel to do the playback.

Note: For more details of PTZ Control and Playback Control, please refer to PTZ Control and Playback sections in this chapter.

8.2. Installing and Starting the SPhone Client on iOS Devices

8.2.1. Installing the SPhone Client (Optional)

Download the SPhone Client from App Store on the iPhone desktop.

8.2.2. Starting the SPhone Client

Note: Please check the web server settings in the SCC Console first.

After the SPhone Client installation is done, a login window will pop up.

- **IP Address**: The IP address for the SCC/NVR Server.
- **Port:** The login port for SPhone Client. **Default port number is *80*.**

Note: The port number should be the same with the web server port.

- **Username** – The username for the domain. **Default username is *admin*.**
- **Password** – The password for the domain. **Default password is *admin*.**

Click **Done** button on the upper right corner after the port, username and password are entered.

8.2.3. Checking the Software Version

Users can see the software version at the lower right corner of the window after logging in.

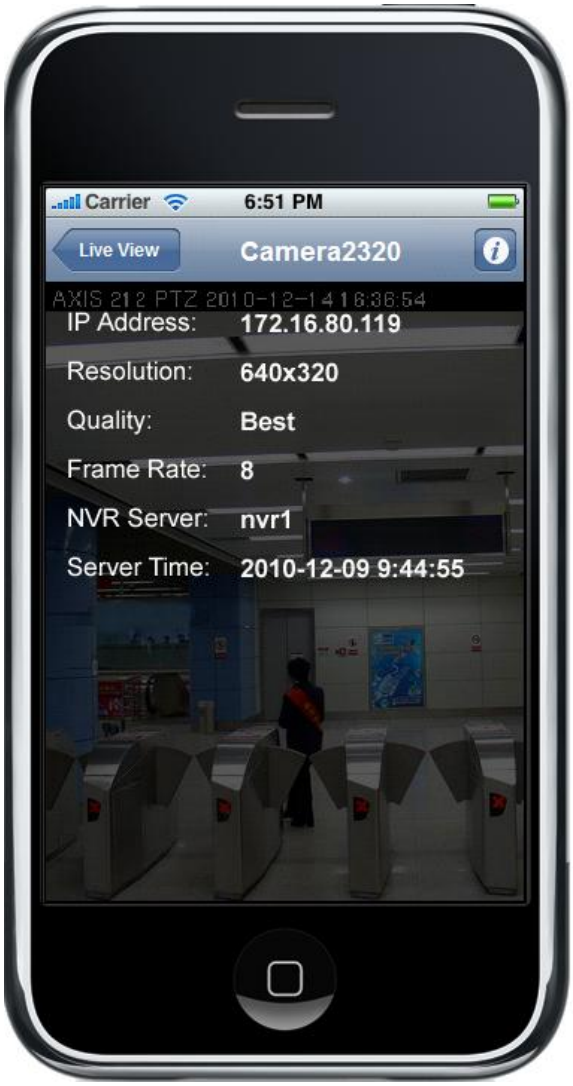
8.2.4. Live View/Playback on the SPhone Client

You can use live view and playback functionalities through SPhone Client:

At most 6-channel live view can be displayed in the same page.

Press the icon at the upper left to jump to the previous page or press the button on the phone to go to the next page.

The icon beside each camera name can be used to check the detailed information of each camera as follows.



- **IP Address:** The IP address for the SCC/SMR Server
- **Resolution:** The video resolution of the camera
- **Quality:** The video quality of the camera
- **Frame Rate :** The frame rate of the camera
- **NVR Server:** The SCC/SMR Server name
- **Server Time**

8.3. Installing and Starting the SPhone Client on Android Devices

8.3.1. Installing the SPhone Client (Optional)

Download the SPhone Client from App Store on the Android phone desktop.

8.3.2. Starting the SPhone Client

Note: Please check the web server settings in the SCC Console first.

After the SPhone Client installation is done, a login window will pop up.

- **IP Address**: The IP address for the SCC/NVR Server.
- **Port:** The login port for SPhone Client. **Default port number is *80*.**

Note: The port number should be the same with the web server port.

- **Username** - The username for the domain. **Default username is *admin*.**
- **Password** - The password for the domain. **Default password is *admin*.**

Click **Done** button on the upper right corner after the port, username and password are entered.

8.3.3. Checking the Software Version

Users can see the software version at the lower right corner of the window after logging in.

8.3.4. Live View on the SPhone Client

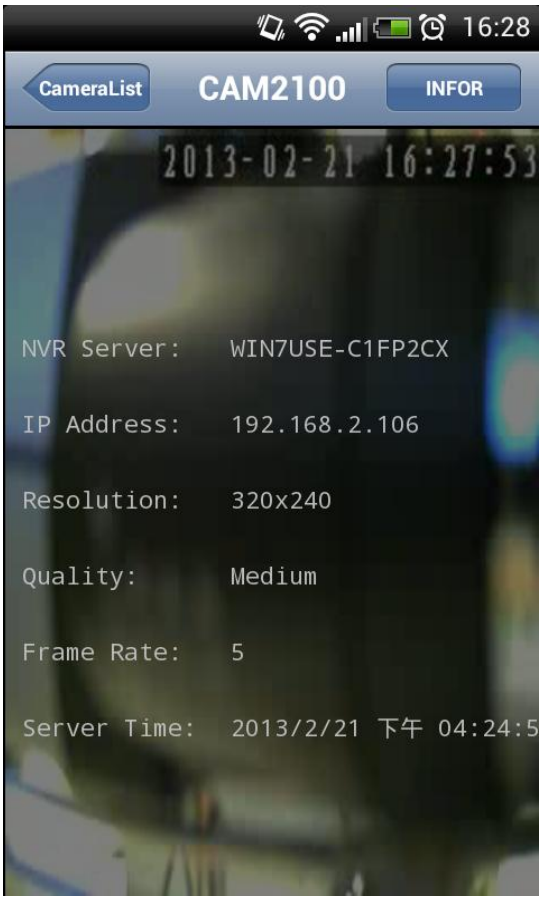
You can use basic live view functionalities through SPhone Client:

At most 6-channel live view can be displayed in the same page.

Press the icon at the upper left to jump to the previous page or press the button on the phone to go to the next page.

The

icon beside each camera name can be used to check the detailed information of each camera as follows.



- **NVR Server:** The SCC/SMR Server name
- **IP Address:** The IP address for the SCC/SMR Server
- **Resolution:** The video resolution of the camera
- **Quality:** The video quality of the camera
- **Frame Rate :** The frame rate of the camera
- **Server Time**

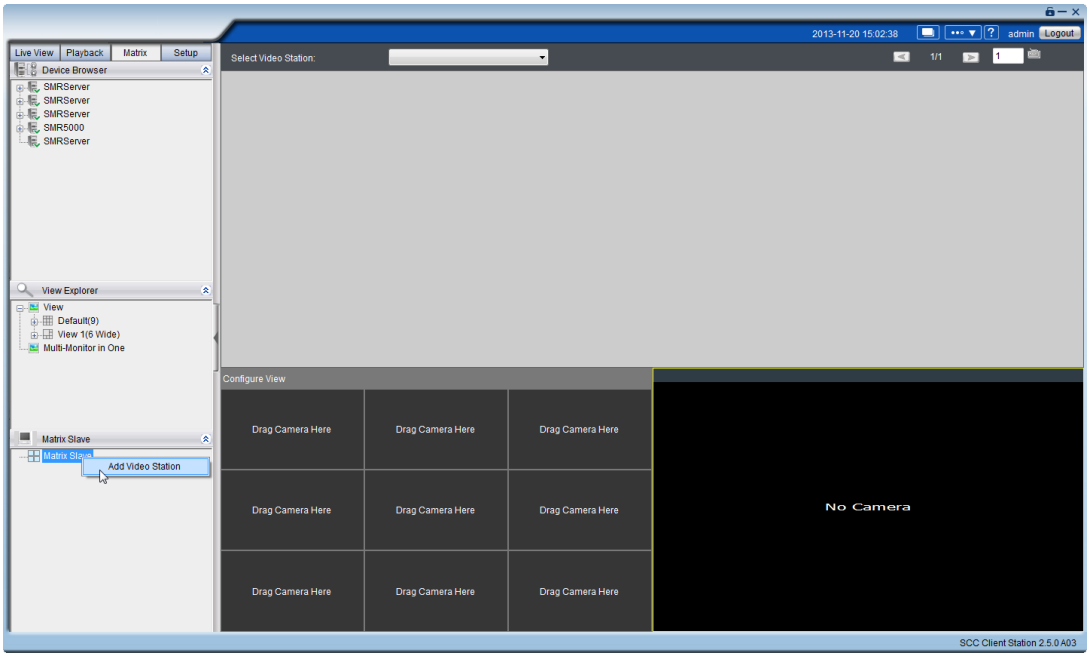
Chapter 9. Matrix Wall Client

9.1. Matrix Slave

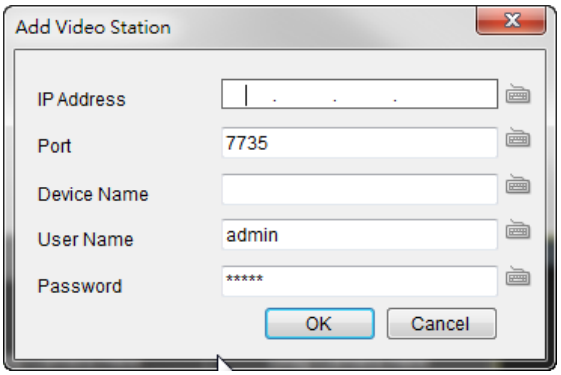
Matrix wall client allows you to add unlimited numbers of cameras and monitors. For each monitor, the screen can be divided up to 6x6 screens.

9.1.1. Add Video Station

Go to the Matrix page, right click the **Matrix Slave** and select **Add Video Station.**



An **Add Video Station** window will be prompted out as below.



4. Input the IP Address of the PC with connected multiple monitors you'd like to display videos on.

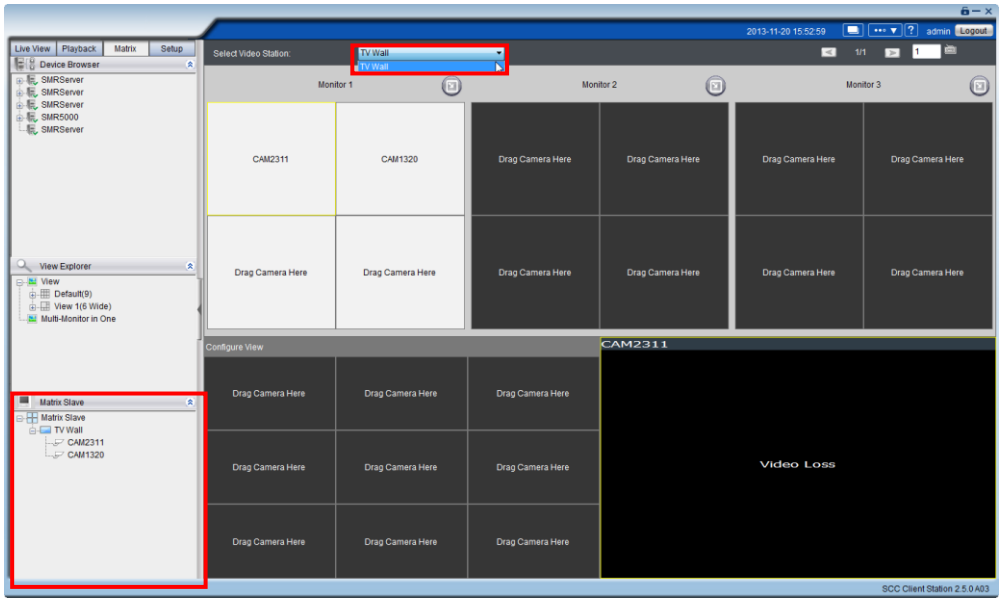
5. Put a description in the Device Name entry.
6. Click OK to confirm and leave this page.

Now you can see the newly added Video Station in the Matrix Slave window.

Repeat the steps above to connect unlimited numbers of PC and monitors to SCC.

Use the dropdown list to select, when there is more than 1 PC connected with SCC.

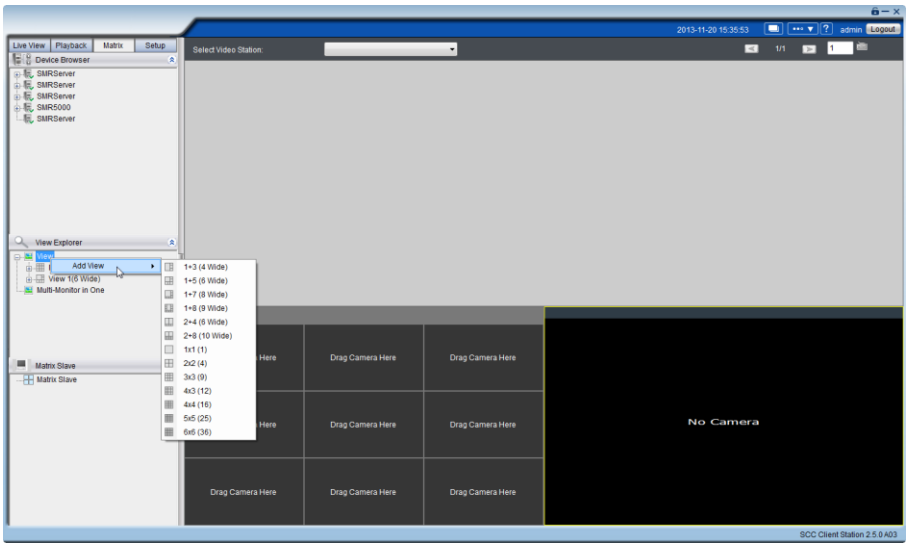
Note: One PC can only be added to one SCC at the same time.



9.2. View Explorer on Matrix Page

9.2.1. View

The numbers of viewing windows can be set in the View Explorer on the Matrix page.

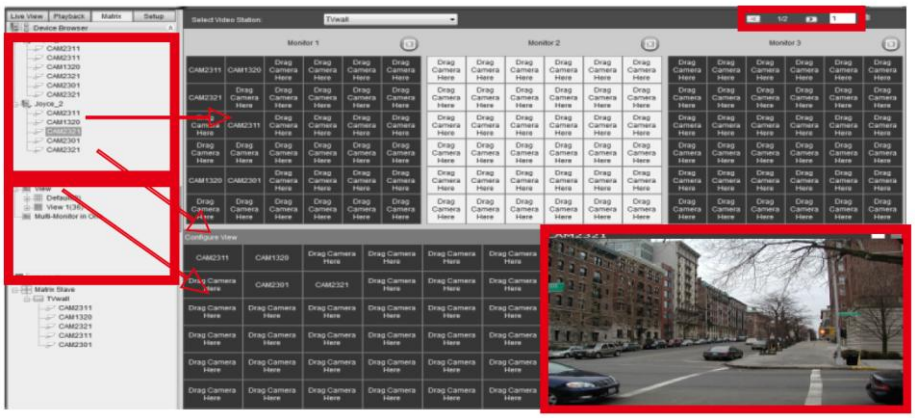


Add View

1. Right click the **View** and click **ADD** to select the numbers of viewing windows you'd like to create on the monitor.

The software responds by placing a blank template in the main viewing window that has been subdivided into individual frames according to the view selected. The empty frames will display the message *No camera*.

2. From the *Device Browser* window, you can drag the cameras from the list on the left directly to the **Monitor** or to the **Configure View** to edit and then drag the whole set **View** to the **Monitor**. Click on the selected camera in the monitor to see its image displayed on the lower right corner window.



The camera output will be displayed in the screen. Cameras can be selected from different server to **View**.

> **Note:** Dragging a camera into a frame that already has a camera assigned to it will cause the frame to be reassigned to the new camera. You can also drag the same camera into multiple frames or leave frames blank.

The *View Explorer* will be updated as you add cameras to your view. The root will list the camera numbers that have been added to the view starting from the top left frame and going from left to right and top to bottom.

> **Note:** Depending on your connection and computer speed, it may take a moment for the image to refresh after dragging the camera into the view window. During this time the frame may still display *No Camera* or *Failed to connect*. If this problem persists, however, there may be a problem with your connection or hardware.

Renaming a View

To perform this function:

1. Right-click the view entry in the *View Explorer* window. This will bring up an options popup.
2. Highlight and click the **Rename** option.
3. Enter a new name for the server and press enter to save the name.

Deleting a View

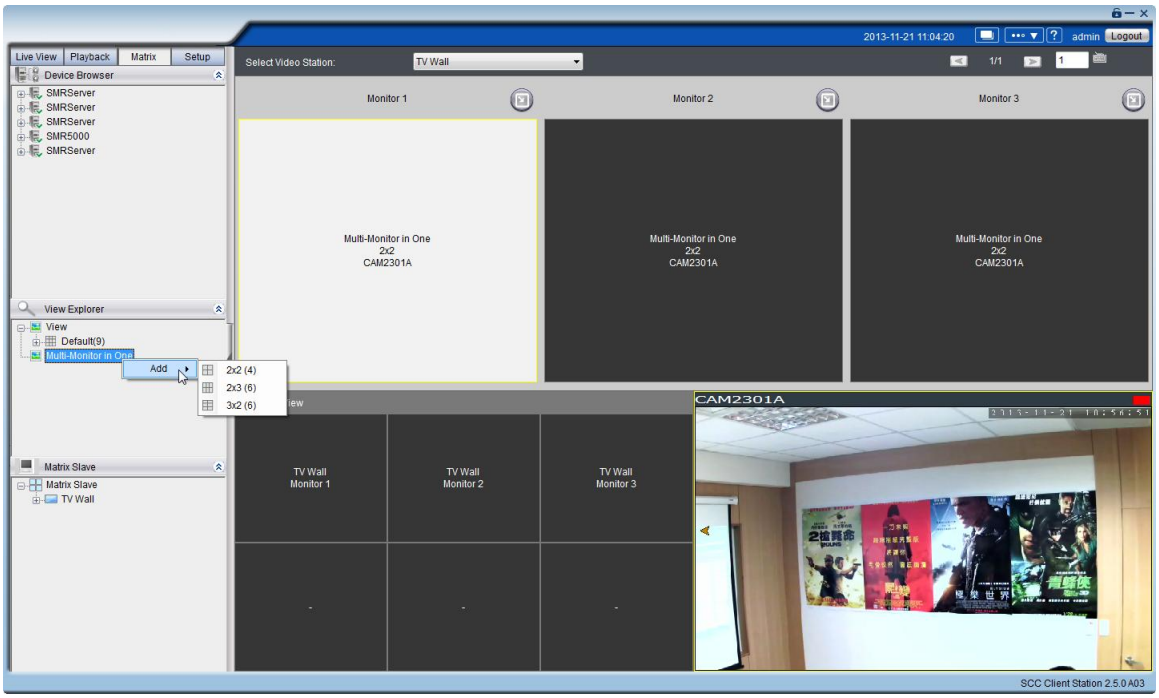
As views become superfluous or unused, it is desirable to delete a view. To perform this function:

1. Right-click the view entry in the *View Explorer* window. This will bring up an options popup.
2. Highlight and click the **Delete** option. The system will respond with a confirmation screen.

Click the **Yes** button to delete the view.

9.2.2. Mutli-Monitor in One (TV Wall)

Multiple monitors can be set as one big screen.

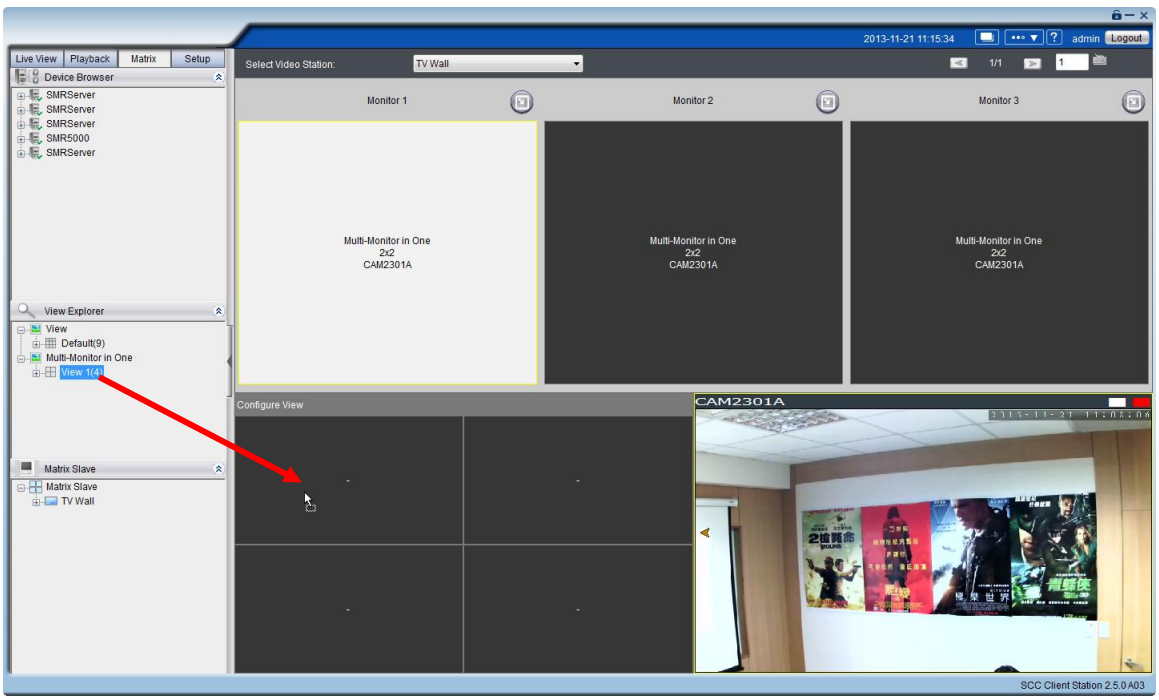


1. Go to View Explorer on the Matrix page.

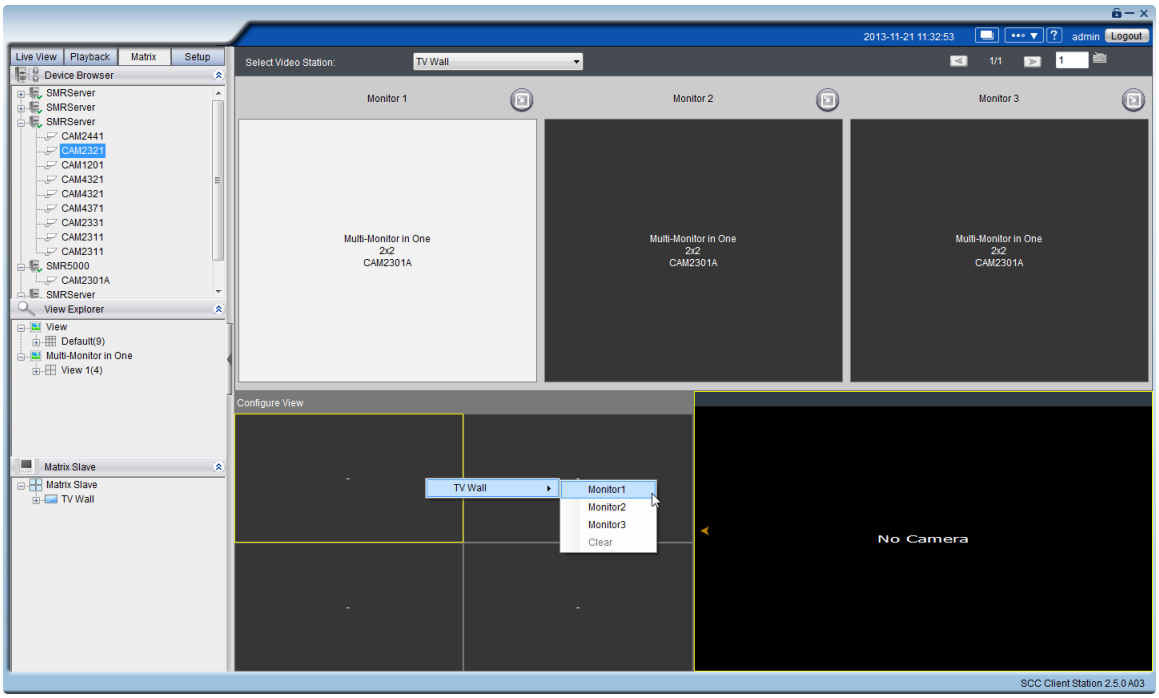
2. Click **Multi-Monitor In One** and click **ADD**.

3. Select the monitor numbers and the way to display, options are 2x2, 2x3 two rows three columns, and 3x2 three rows two columns.

4. Once set, drag the whole newly added **View** to the **Configure view.**

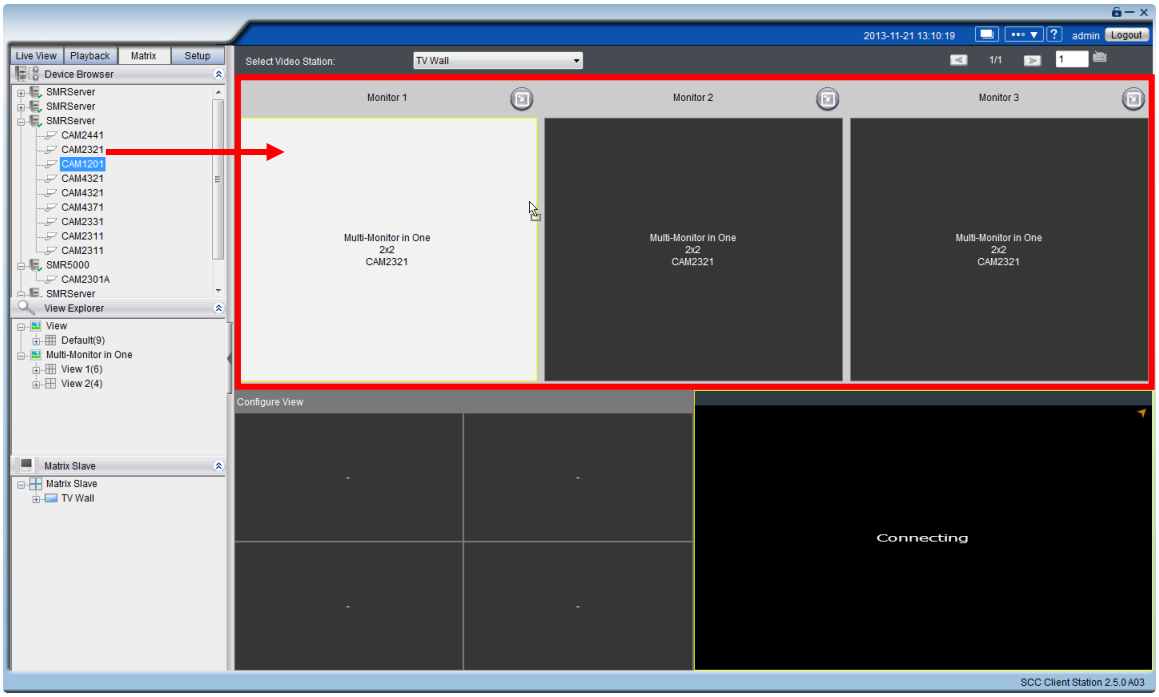


3. Select and right click on any screen of the Configure View to arrange the order of the monitors.

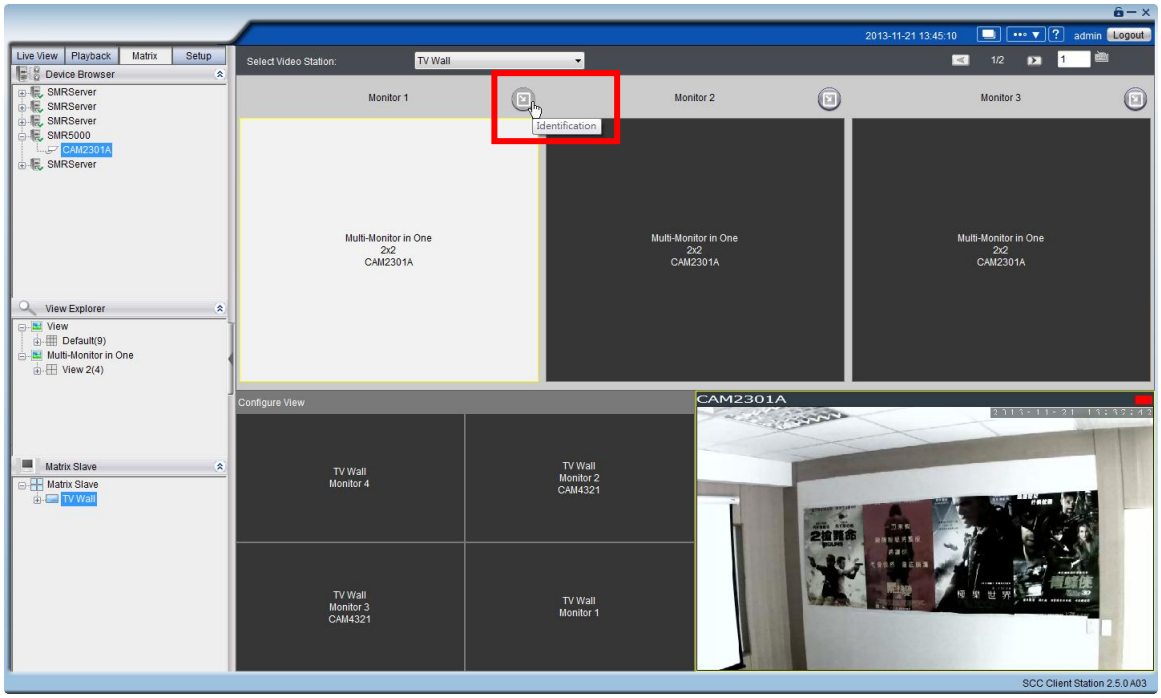


3. Repeat step 2 to complete the monitor order setting. After the monitor order setting, you will see Monitor 1(~6) showing Multi-Monitor in One.

4. Now drag the camera you'd like to display in one big TV wall to any one of the upper screen.



Use the identification button to identify which display is Monitor 1.

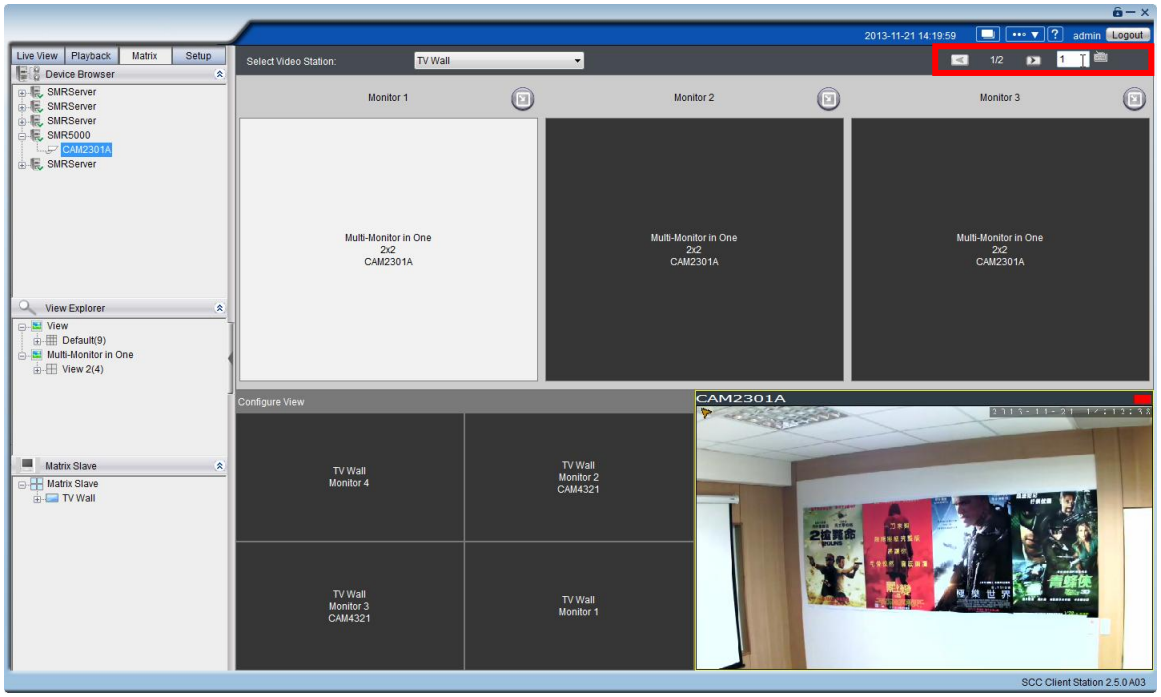


When clicking on the identification button of the Monitor 1, the display representing Monitor 1 will flash with the number 1, so that the monitor order can be checked.

When the monitor order is not right, just repeat step 3 to rearrange the order and use the identification button to check.

Screen Division Page Use

The page number is on the upper right corner of the page. Clicking on the arrow button to the next or previous page or simply input the page number.

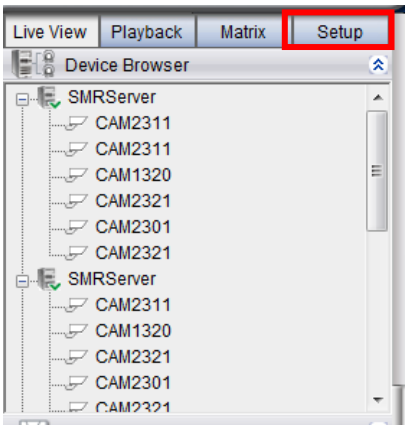


Chapter 10. System Setup

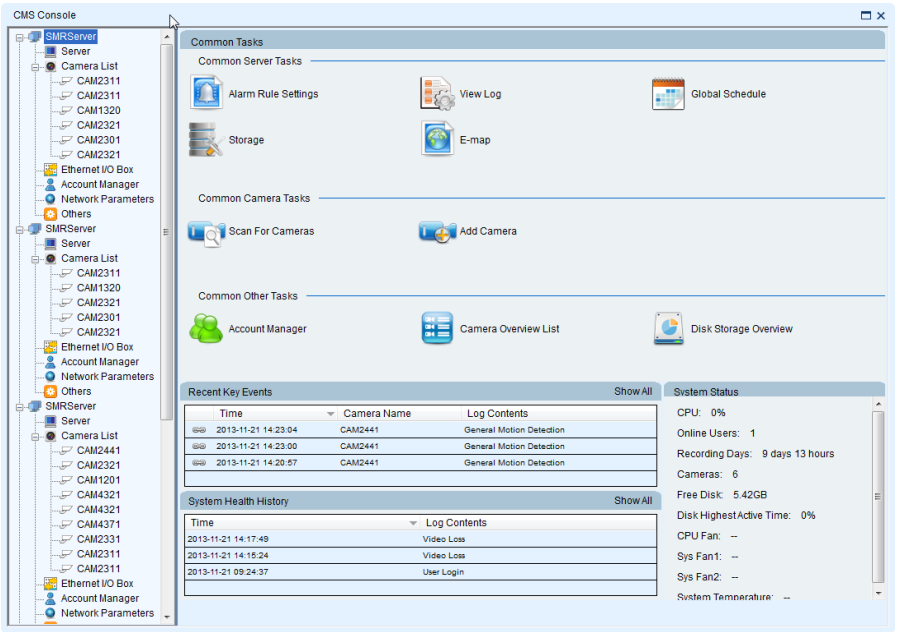
10.1. Settings Under SMR / NVR Server

In the SCC system, the management scope is referred to as a “Domain.” Managed servers are all part of a “Domain” with uniform access rules and a single configuration point. For basic local domains this configuration points are the SCC Console.

Select Setup Button on the menu bar.



The SCC Console under SMR / NVR Server shows up listing shortcuts to commonly used functionalities, system status, and recent events.



Common Server Tasks

Lists shortcuts to frequently accessed server functionalities.

Alarm Rule Settings

In the alarm rule settings, you can combine the alarm trigger conditions with action items such as event notification, video recording, and/or camera movements. See *Alarm Rules* for more details.

View Log

The Event Log displays the camera the alarm occurred on, the date, the alarm type, and if applicable a link to the live-view feed of the camera. See *Alarms View and Notification* > *Live View Event Log* for more details.

Global Schedule

A global schedule can be created to apply to an entire Server. See *Scheduling Recording* > *Global Scheduling* for more details.

Storage

Opens the Storage Manager that allows you to configure storage settings. See *Server Settings* > *Storage Management* for more details.

E-map

When alarms occur, an administrator can quickly locate where the alarms took place using an E-map. See *E-Maps* for more details.

Common Camera Tasks

Lists shortcuts to frequently accessed camera functionalities.

Scan for Cameras

Allows you to scan cameras automatically. See *Adding Cameras* > *Automatic Scan for Cameras* for more details.

Add Cameras

Allows you to add cameras manually. See *Adding Cameras* > *Manually Adding Cameras* for more details.

Common Other Tasks

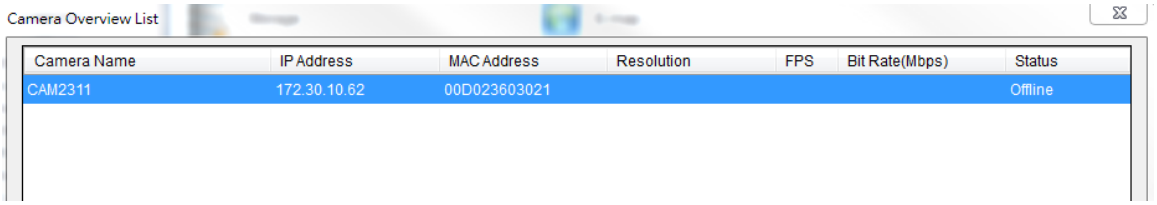
Lists shortcuts to frequently accessed system tasks.

Account Manager

Allows you to manage user accounts. See *Account Manager* for more details.

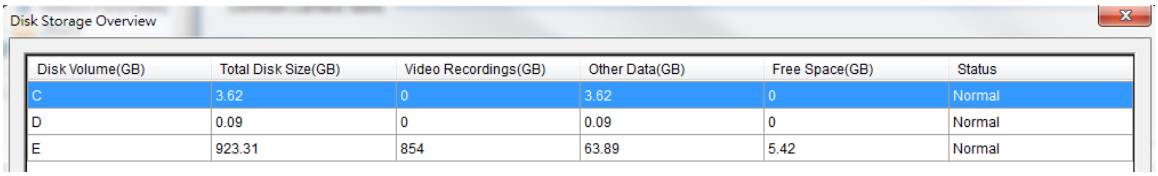
Camera Overview List

Shows the cameras added and their status.



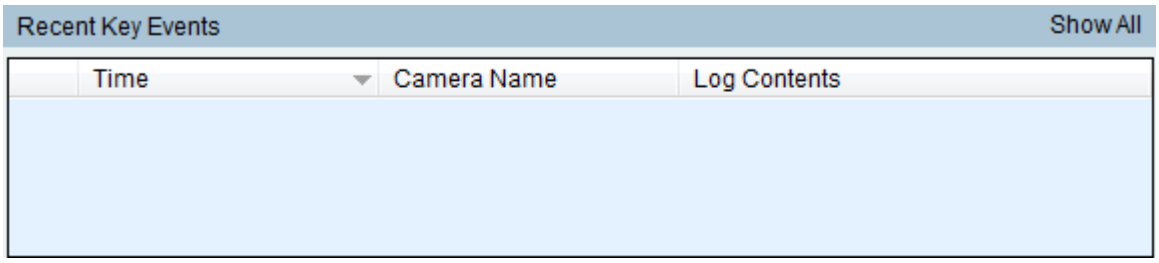
Disk Storage Overview

Shows information about the hard disks.



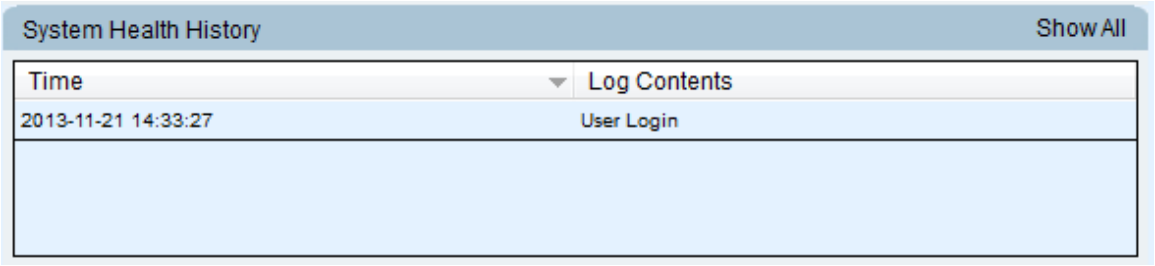
Recent Key Events

Lists recent important system events. To view all system events, click Show All at the top right corner. The Event Log will appear. See *Alarms View and Notification* > *Live View Event Log* for more details.



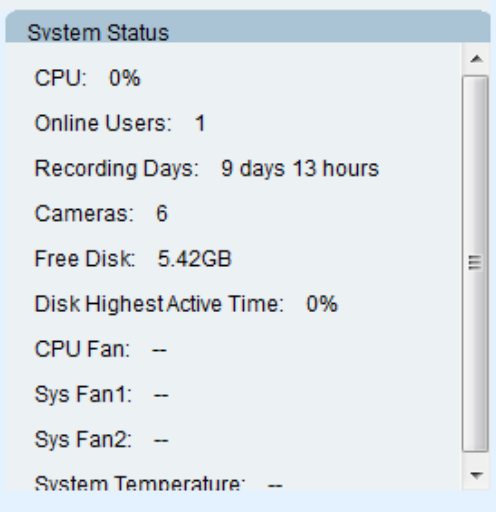
System Health History

Lists the summary of recent user access. To view all history, click Show All at the top right corner.



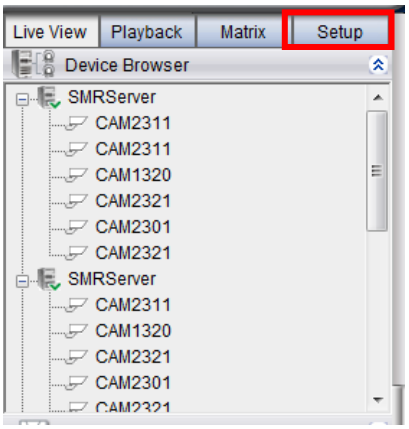
System Status

Shows the status of system components.

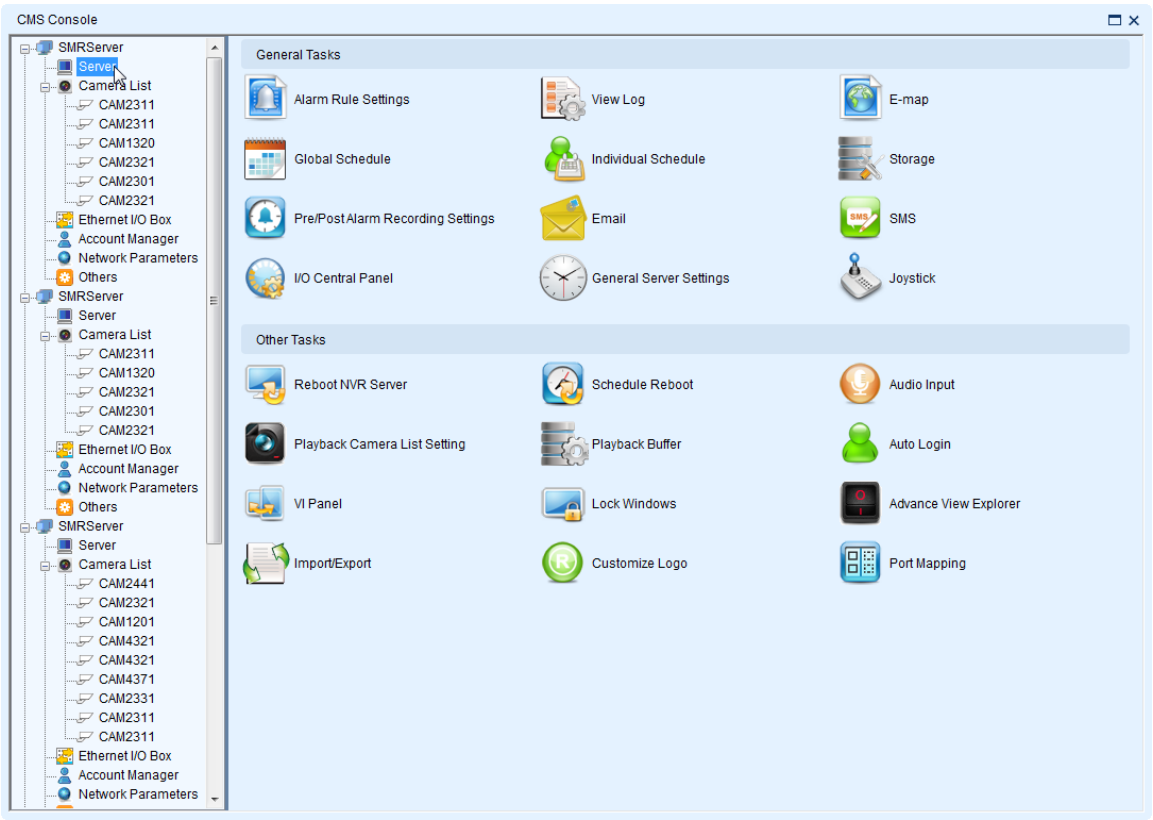


10.2. Settings Under Server

Select Setup Button on the menu bar.

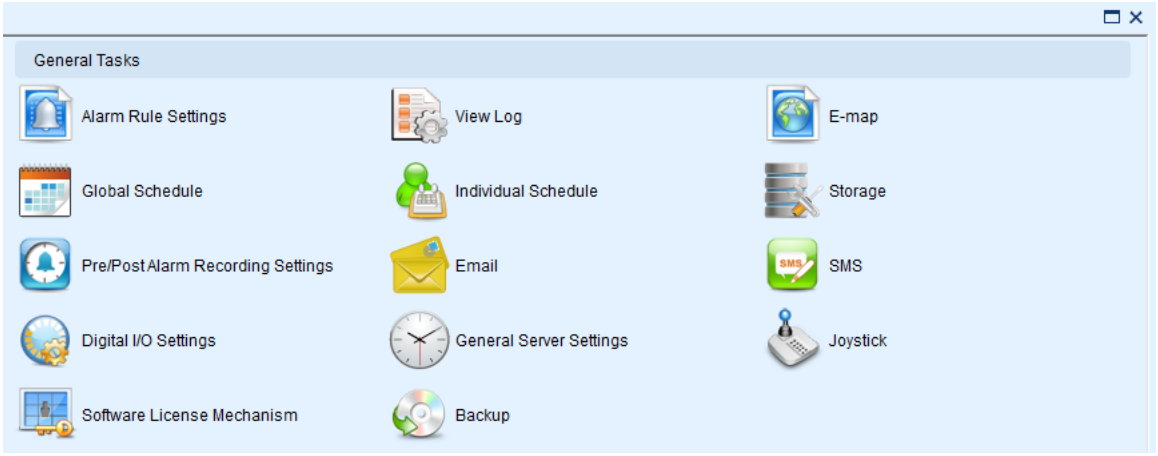


The SCC Console under Server shows up listing General Tasks and Other Tasks.



10.2.1. General Tasks

Here you can access shortcuts for general server settings.



Alarm Rule Settings

In the alarm rule settings, you can combine the alarm trigger conditions with action items such as event notification, video recording, and/or camera movements. See *Alarm Rules* for more details.

View Log

The Event Log displays the camera the alarm occurred on, the date, the alarm type, and if applicable a link to the live-view feed of the camera. See *Alarms View and Notification* > *Live View Event Log* for more details.

E-Map

When alarms occur, an administrator can quickly locate where the alarms took place using an E-map. See *E-Maps* for more details.

Global Schedule

A global schedule can be created to apply to an entire Server. See *Scheduling Recording* > *Global Scheduling* for more details.

Individual Schedule

Individual schedules, which take precedence over the global schedule, can be set for each camera. See *Scheduling Recording* > *Individual Scheduling* for more details.

Storage

Opens the Storage Manager that allows you to configure storage settings. See *Server Settings* > *Storage Management* for more details.

Pre/Post Alarm Recording Settings

The Server can trace back and preserve video/images from several minutes before and after the occurrence of an alarm. See *Server Settings* > *Pre/Post Alarm Recording Settings* for more details.

Email

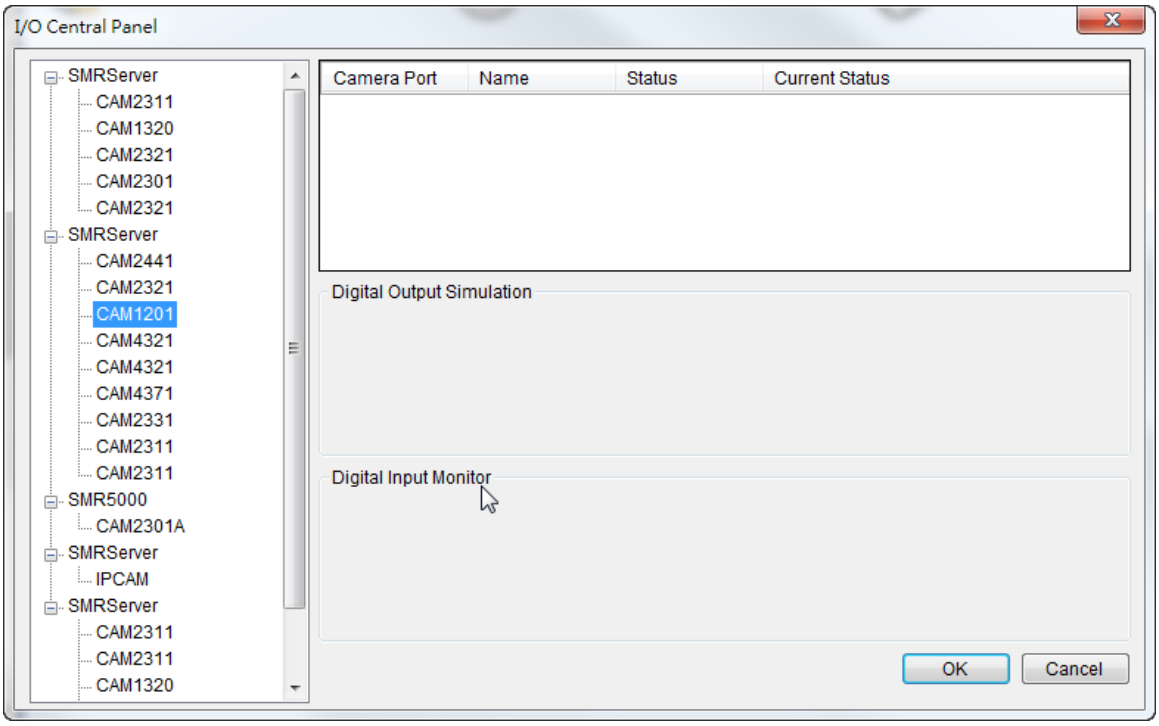
When the alarm is triggered, an E-Mail will be sent. See *Alarm Rules*> *Alarm Actions* > *Email* for more details.

SMS

Configures the SMS setting. See *Server Settings* > *To perform Notification Setting* for more details.

I/O Central Panel

Allows you to configure digital I/O port settings.

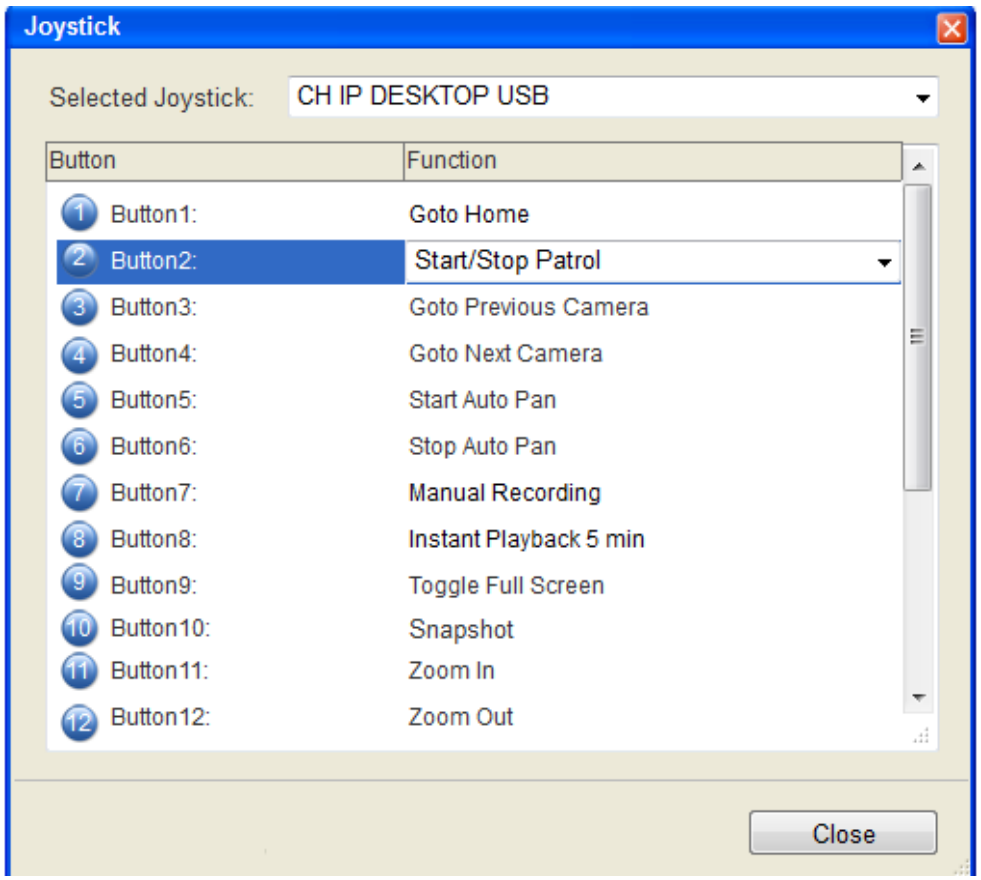


Genera Server Settings

Involves configuring storage quota, server time settings and automatic correction. See *Server Settings* > *General Server Settings* for more details.

Joystick

CH Products IP Desktop USB Joystick is supported for PTZ camera control. Connect the joystick controller to the USB port. The *Joystick Settings* Window will prompt after clicking **Joystick**. In this window, functions of each button are listed.



Button Number	Function
1	Resets all the settings, including page auto-flipping and different screen divisions.
2	Switches on/off the functionality of switching between preset viewpoints.
3	Goes to the view of the previous camera.
4	Goes to the view of the next camera.
5	Starts auto pan.
6.	Stops auto pan.
7	Manually records the video streams.
8	Pops up an instant playback for five minutes.

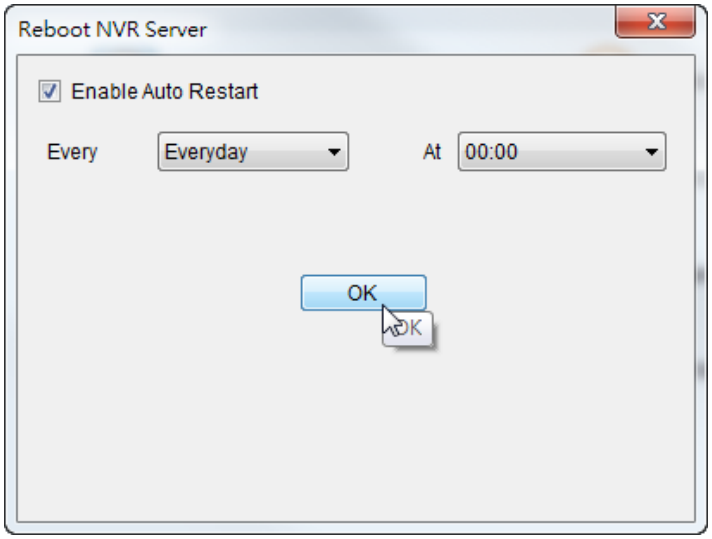
9	Brings up the full screen view.
10	Captures a snapshot.
11	Increase the zoom distance.
12	Decrease the zoom distance.

You may reset the functions by choosing within the dropdown list.

10.2.2. Other Tasks

Here you can access shortcuts for advanced server settings.

Reboot NVR Server

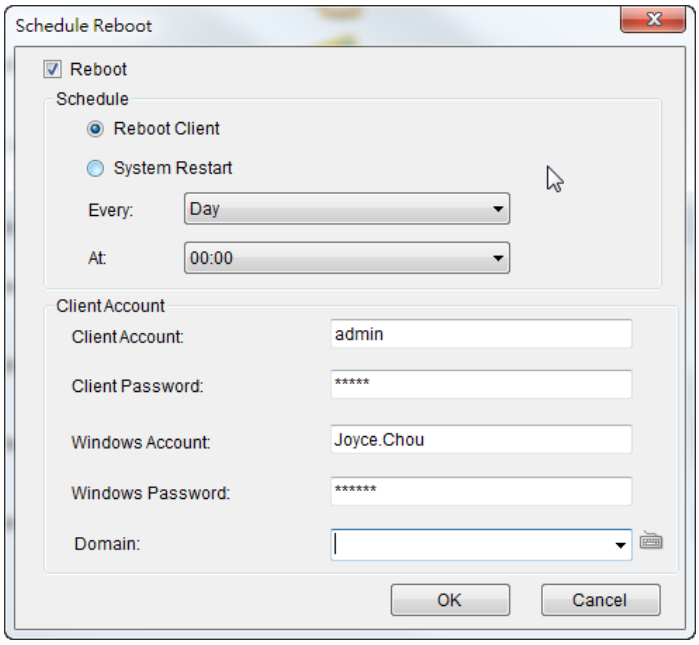


The Server can be configured to perform a scheduled restart, daily or on a certain day of the week. Due to the trend of Windows performance degradation over time, we recommend that a reboot be performed at least once a week. This function can be found in the *Auto Reboot* node of the *Server*.

To configure an auto restart in this menu:

1. Select the **Enable Auto Restart** checkbox.
2. From the **Every** dropdown choose a day which you want to schedule an automatic restart. Options include weekly (Monday – Sunday) or Daily restarts.
3. From the **At** dropdown, choose the hour which you want to perform the restart. Options include every hour of the day.
4. Click the OK button to save your settings.

Schedule Reboot



The client can be setup to automatically restart the client or the computer.

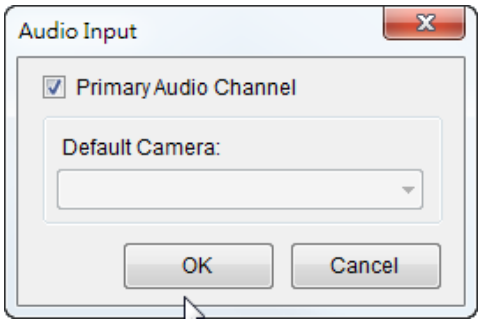
To configure the auto-reboot function:

1. From the client Schedule Reboot popup, check the **Reboot** box.
2. Select either **Reboot Client** to schedule a client restart, or **System Restart?** to schedule a windows restart.
3. From the **Every** dropdown, choose the day that you want to schedule restarts, or you may choose to restart every day.
4. From the **At** dropdown, choose the scheduled restart time.

Note: Auto-Login should be configured with Auto-restart or you will lose functionality until a user can be logged-in.

Audio Input

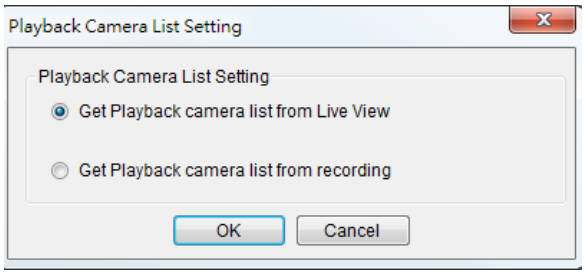
There are two choices available for audio channel selection. These two are selected using the **Primary Audio Channel** check box. If checked, the client will automatically use the audio feed from the selected/highlighted camera during live view.



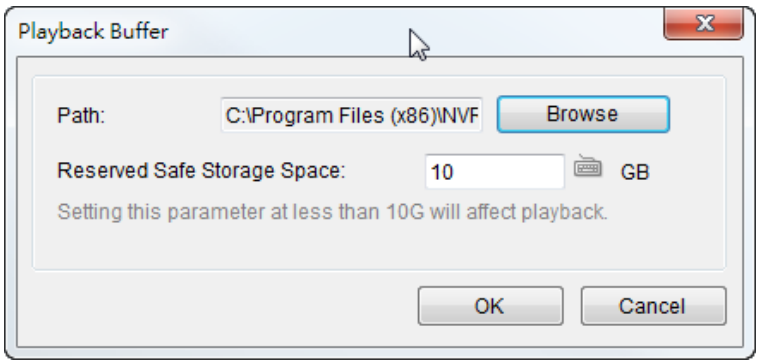
Unchecking the box will allow you to select a camera from the **Default Camera** drop-down. This camera will provide the audio feed no matter which channel is selected in live-view.

Playback Camera List Setting

Playback camera list can be from Live View or from the recording.

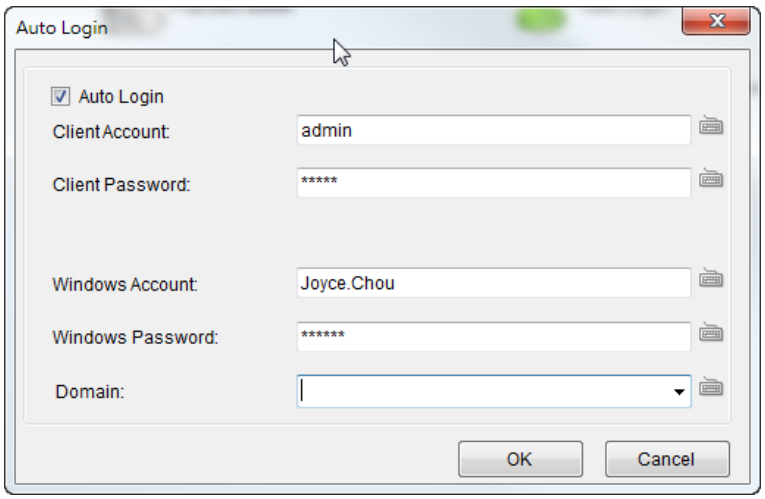


Playback Buffer



The Playback Buffer is used for downloading video recordings before the playback. The reserved safe storage space should be at least 10 GB.

Auto Login



The client can be setup to automatically login after a crash or on startup.

To configure the auto-login function:

1. From the client general settings popup, check the **Auto Login** box.
2. If you want to automatically login to the client, enter the following information:
   - **Client Account** – The client account name.
   - **Client Password** – The client password.
3. If you want to automatically log into windows after a restart enter the following information:
   - **Windows Account** – The Windows account name.
   - **Windows Password** – The Windows password.
   - **Domain** – The login domain.

VI Panel

Open or close VI Panel on the main screen to display the alarm-triggered images and adjust the display windows in either 16:9 or 4:3 aspect ratios via clicking **VI Panel**.

Lock Windows

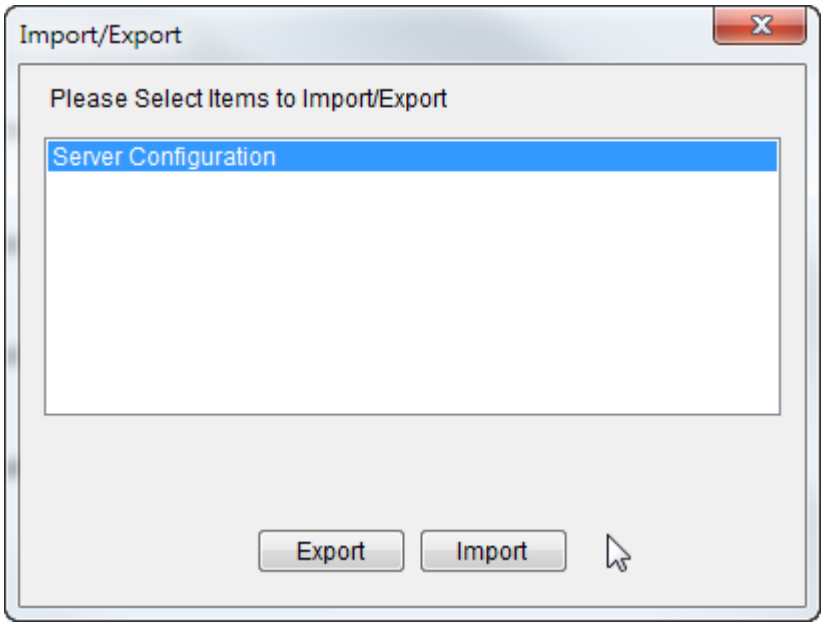
The Video Panels can be locked by clicking **Lock Windows**.

Advance View Explorer

View Explorer on the Live View page can be opened or closed by clicking this button.

Import/Export

The following types of configuration/setup files can be imported/exported to the Server:



- **Server Configuration**

Importing Parameters

To import parameters into the Server:

1. Select the item that you wish to import by clicking on the item type.
2. Click the **Import** button. A windows explorer dialog will appear.
3. Select the file to import from the file explorer, and click **Open** to import the file.
4. Click **OK** to confirm import. The Server will require a restart before imported configurations and files are applied.

Exporting Parameters

To export parameters into the Server:

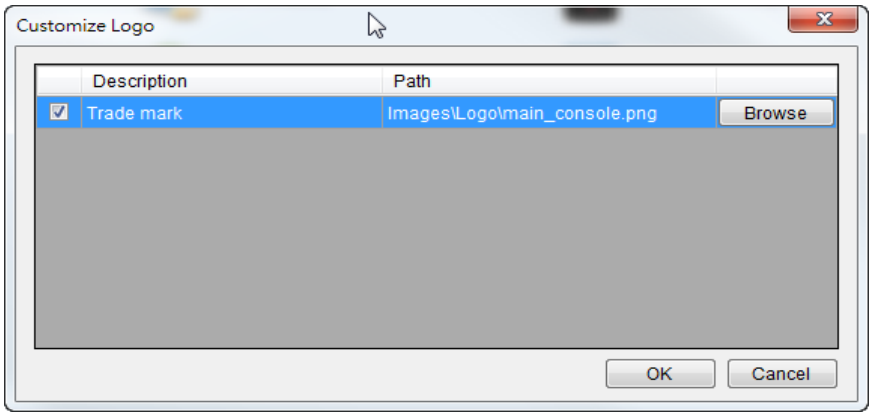
1. Select the item that you wish to export by clicking on the item type.

2. Click the **Export** button. A windows explorer dialog will appear.

3. Input a filename and select the export path in the file explorer, and click **Save** to export the file.

Customize Logo

Allows users to change the logo by using the "Browse" and selecting a customized logo file.

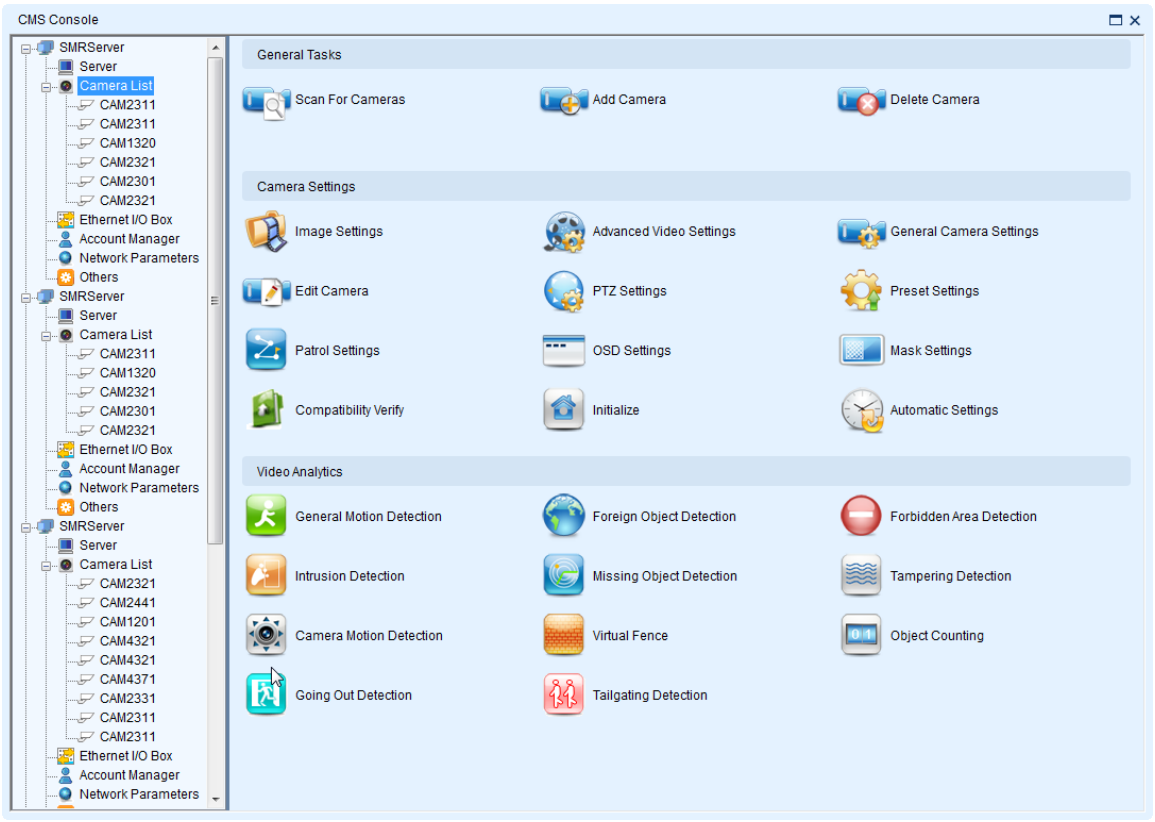


Note: The recommended size for the logo pictures is 280X52, in png format.

Router Port Mapping

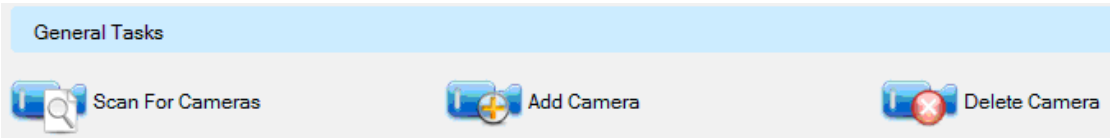
Router Port Mapping for SCC/NVR Server. See *Port Forwarding > Port Forwarding for Accessing SCC Server* for more details.

10.3. Settings Under Camera List



10.3.1. General Tasks

Here you can access shortcuts for general camera settings.



Scan for Cameras

Allows you to scan cameras automatically. See *Adding Cameras* > *Automatic Scan for Cameras* for more details.

Add Cameras

Allows you to add cameras manually. See *Adding Cameras* > *Manually Adding Cameras* for more details.

Delete Camera

Allows you to delete cameras manually. See *Deleting a Camera* for more details.

10.3.2. Camera Settings

Here you can access shortcuts for general camera settings.

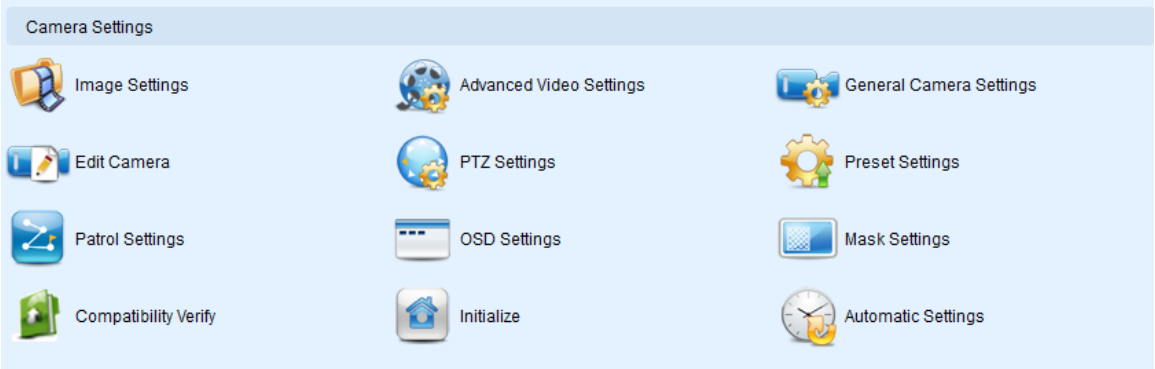


Image Settings

Allows you to adjust camera image settings. See *Camera Image and Quality Settings > Camera Image Settings* for more details.

Advanced Video Settings

Allows you to adjust video image parameters. See *Camera Image and Quality Settings > Advanced Video Settings* for more details.

General Camera Settings

Camera general settings include network connectivity settings, as well as basic camera name, description and icon settings. See *Camera General Settings > General Settings* for more details.

Edit Camera

In certain situations it may be necessary to change the Vendor or Model information for the camera. See *Camera General Settings > Changing the Camera Model and Vendor* for more details.

PTZ Settings

The PTZ settings deal with the software PTZ control panel. These settings adjust how much the camera will pan, tilt, zoom, and focus with each control panel input. See *PTZ Settings > PTZ Settings* for more details.

Preset Settings

Certain preset pan/tilt/zoom values can be saved in order to move the camera quickly to a point of interest. See *PTZ Settings* > *PTZ Preset Settings* for more details.

Patrol Settings

In cameras with PTZ functionality, one camera can be used to survey a large area. This can be done automatically using the patrol functionality. See *PTZ Controls* > *Patrol* for more details.

OSD Settings

On cameras with OSD capabilities, these capabilities can be configured within the server. See *Camera General Settings* > *OSD Settings* for more details.

Mask Settings

The camera can be configured to display useful information on the top bar. See *Camera General Settings* > *Privacy Mask Settings* for more details.

Compatibility Verify

Check the compatibility of other connecting device.

Initialize

Restores initial settings of the camera. See *Initializing a Camera* for more details.

Automatic Settings

Camera time can be synchronized with the server. See *Camera Settings* for more details.

10.3.3. Video Analytics

Here you can access shortcuts for VI functions.

General Motion Detection

General motion detection involves using the software to analyze the video feed and detect motion in specified areas. See *Camera VI Detection Settings* > *General Motion Detection* for more details.

Foreign Object Detection

Foreign object detection involves using the software to analyze a video feed and detect objects that do not belong. See *Camera VI Detection Settings* > *Foreign Object Detection* for more details.

Forbidden Area Detection

Forbidden area detection involves using the software to analyze the video feed and immediately detect any object in specified areas. See *Camera VI Detection Settings* > *Forbidden Area Detection* for more details.

Intrusion Detection

Intrusion detection involves using the software to analyze the video feed and detect intrusion in specified areas. See *Camera VI Detection Settings* > *Intrusion Detection* for more details.

Missing Object Detection

Missing object detection involves using the software to analyze the video feed and detect missing objects larger than a certain size. See *Camera VI Detection Settings > Missing Object Detection* for more details.

Tampering Detection

Tampering detection involves using the software to determine when the camera has been improperly moved or redirected. See *Camera VI Detection Settings > Tampering Detection* for more details.

Camera Motion Detection

Camera motion detection involves using the camera hardware to analyze the video feed and detect motion in specified areas. See *Camera VI Detection Settings > Camera Motion Detection* for more details.

Virtual Fence

Virtual fence involves using the software to create a fence-crossing detection of the demanding object. See *Camera VI Detection Settings > Virtual Fence* for more details.

Object Counting

Object counting involves using the camera to count demanding object crossing the fences. See *Camera VI Detection Settings > Object Counting* for more details.

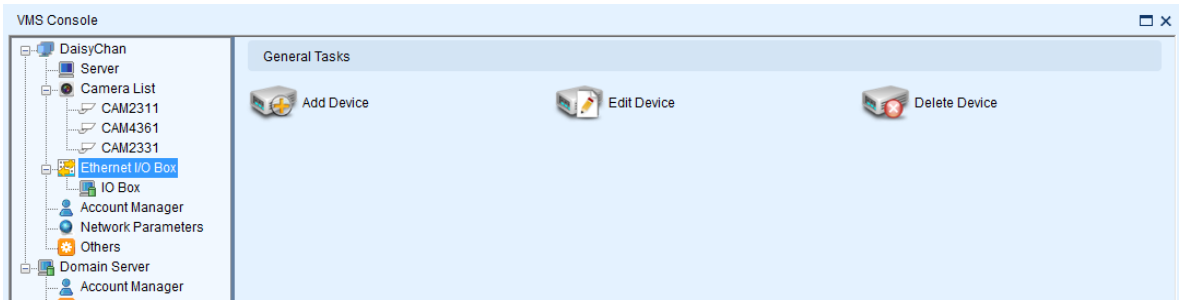
Going Out Detection

Camera motion detection involves using the camera hardware to analyze the video feed and detect motion in specified areas. See *Camera VI Detection Settings > Going Out Detection* for more details.

Tailgating Detection

Camera motion detection involves using the camera hardware to analyze the video feed and detect motion in specified areas. See *Camera VI Detection Settings > Tailgating Detection* for more details.

10.4. Settings Under Ethernet I/O Box

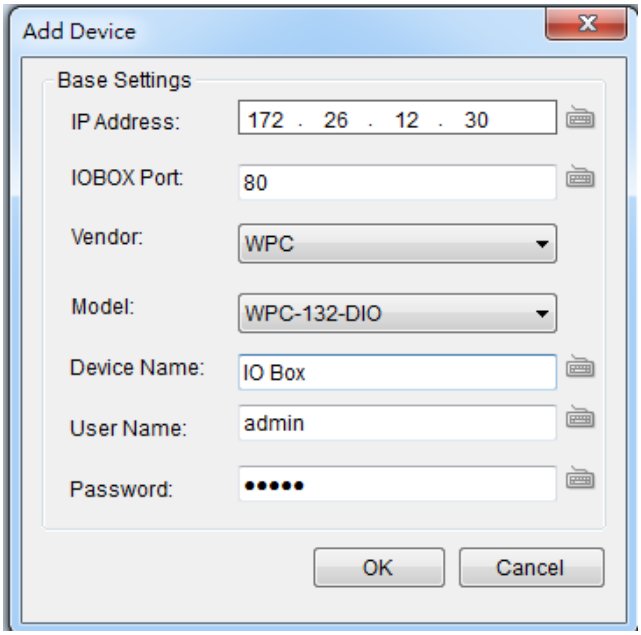


10.4.1. General Tasks

Here you can access shortcuts for general I/O box settings.

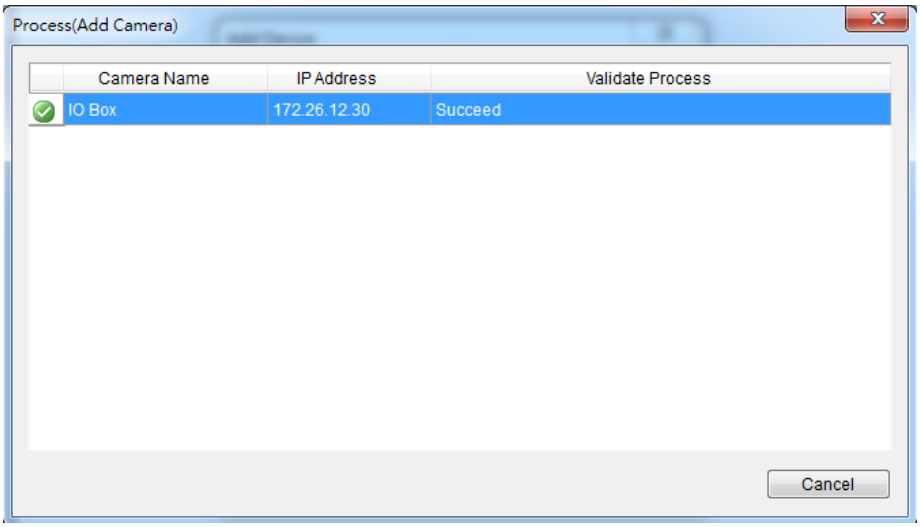
Add Device

Allows you to add Ethernet I/O box to the server.



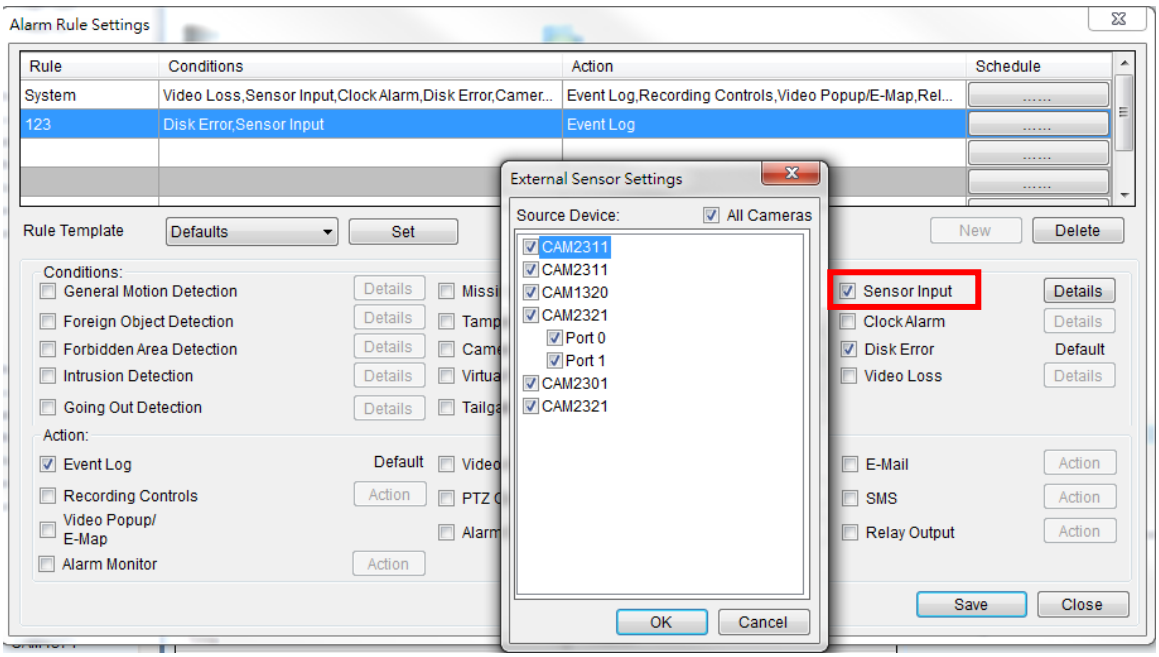
- **IP Address:** The default IP for the I/O box, which is 192.168.0.100.
- **I/ O Box Port:** 80.
- **Vendor:** WPC
- **Model:** WPC-132-DIO.
- **Device Name:** Enter the device name as you like.
- **User Name:** Same with SCC username, **which is always admin**.
- **Password**: Same with the password for SCC login.

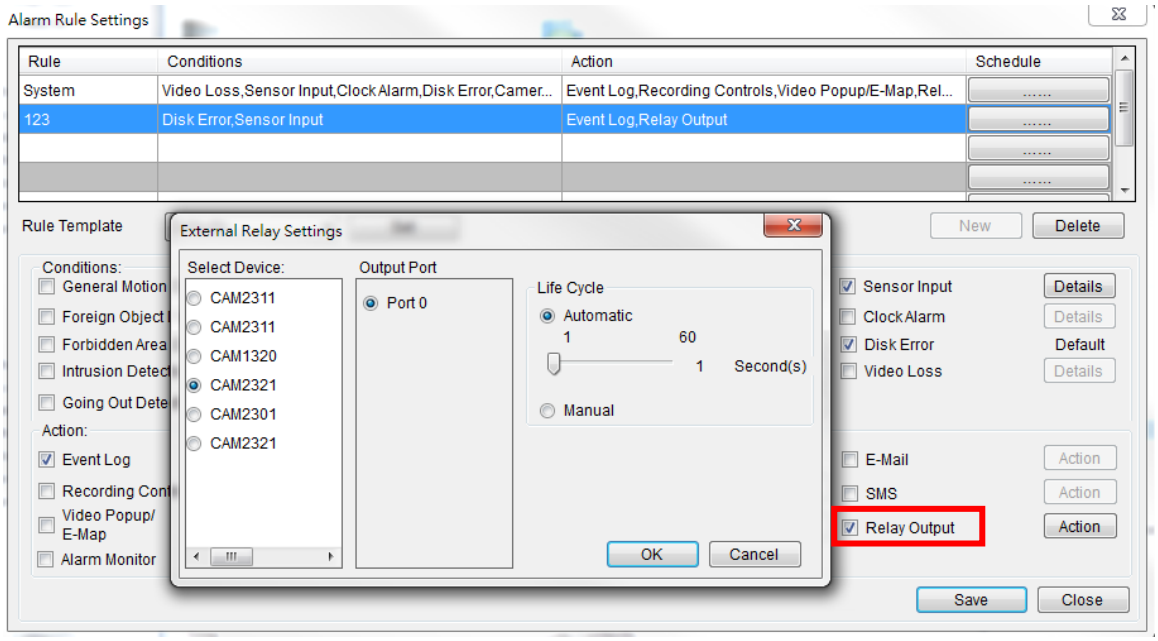
After the I/O box is added successfully, it will appear on the device list.



Go to Alarm Rule Setting under SMR Server, and set Senor Input and Relay Output.

Choose the input/output port numbers.





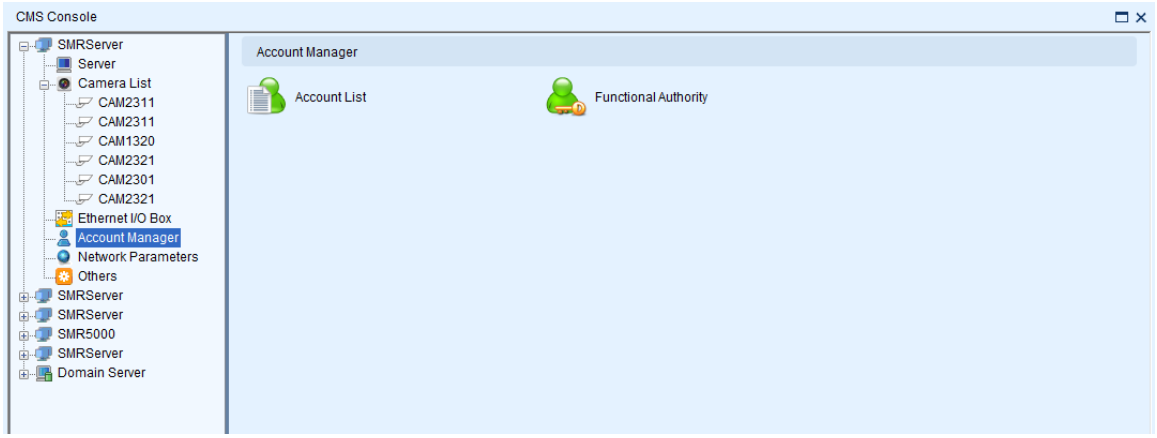
Edit Device

Allows you to edit the added I/O box.

Delete Device

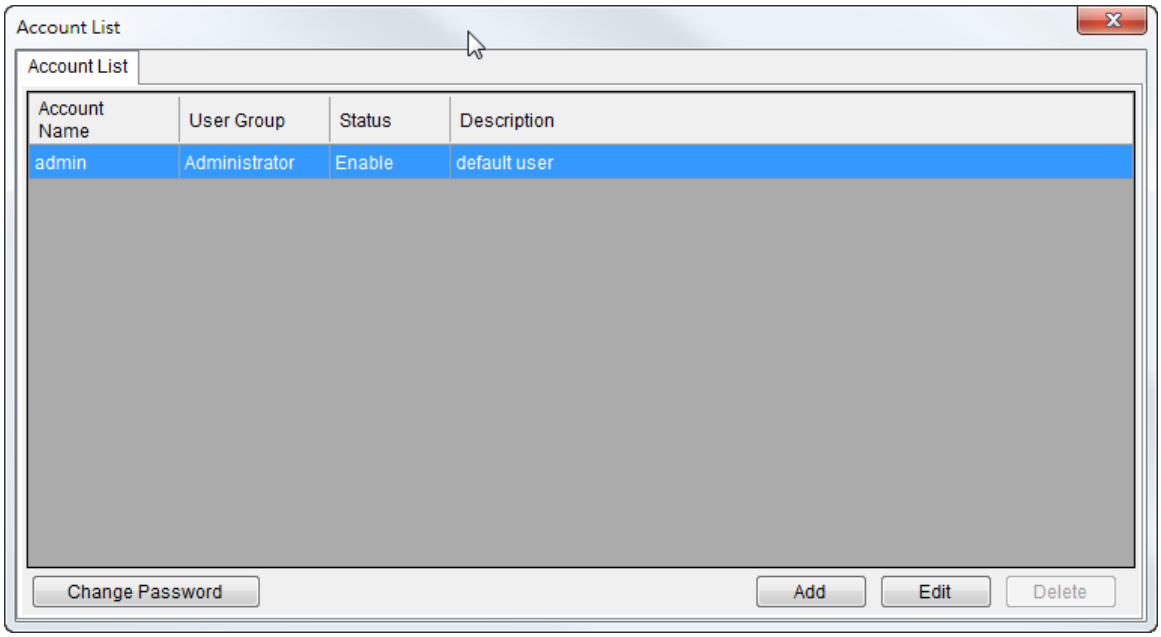
Allows you to delete the added I/O box.

10.5. Settings Under Account Manager



10.5.1. Account List

Account management for the domain can be performed under the *Account Manager* > *Account List* node in the *SCC Console*. Under this dialog, you may add, delete, and edit domain users.



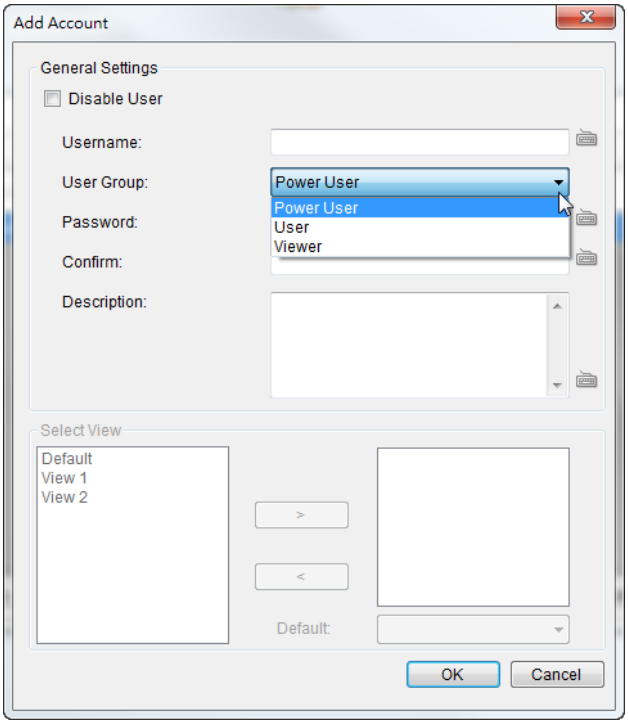
The *Account List* provides the following information about each account:

- **Account Name**
- **User Group** - Type for this user.
- **Status** - This shows if the user is disabled or enabled.
- **Description** - A simple description of the user.

Adding an Account

To add an account to the domain:

1. Access the *Account List* node in the *SCC Console*.



2. Click the **Add** button at the bottom of the *Account List* screen.

3. In the resulting screen fill out information for the new account:
   - **Username**
   - **User Group -** Select a user type for this user. There are 3 types:
     - **Power User** – This group has complete account management rights, but does not have many SCC/Server configuration rights.
     - **User** – This group has no configuration rights and limited SCC/Server performance statistics.
     - **Viewer** – This group is limited only to viewing, and has no access to configuration or performance statistics.
   - **Password / Confirm Password** – The password must be typed twice for confirmation purposes.
   - **Description** – A simple description of the new user.

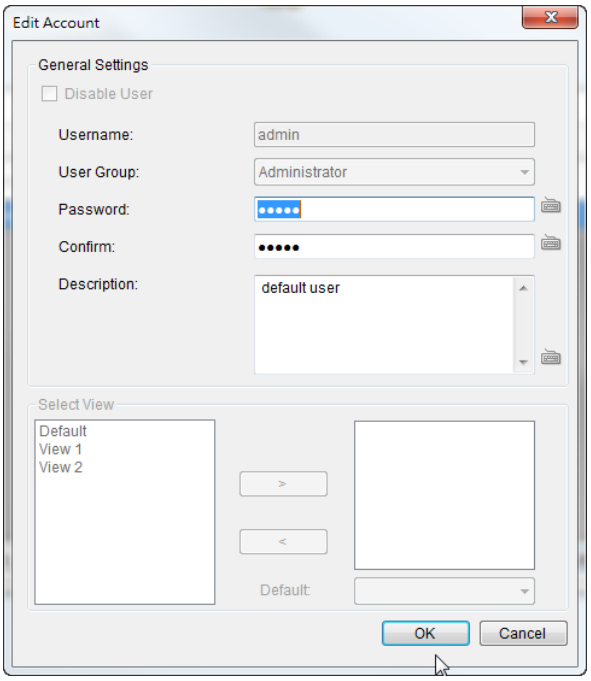
4. When needed, check the **Disable User** box to disable this account.

   Click **Ok** to add the new account. The account will appear in the *Account List*.

Editing an Account

To edit an account to the domain:

1. Access the *Account List* node in the *SCC Console*.
2. Select the account that you wish to edit by clicking on the account.



3. Click the **Edit** button at the bottom of the *Account List* screen.
4. In the resulting screen change any of the following account information:

   - **User Group -** Selects a user type for this user. There are four options:
     - **Administrator** – This group has complete management privileges, including account and SCC/NVR Server management rights.
     - **Power User** – This group has complete account management rights, but does not have many SCC/NVR Server configuration rights.
     - **User** - This group has no configuration rights and limited SCC/Server performance statistics.
     - **Viewer** – This group is limited only to viewing, and has no access to configuration or performance statistics.

   - **Password/Confirm Password** – If changed the password must be typed twice for confirmation purposes.
   - **Description -** A simple description of the user.

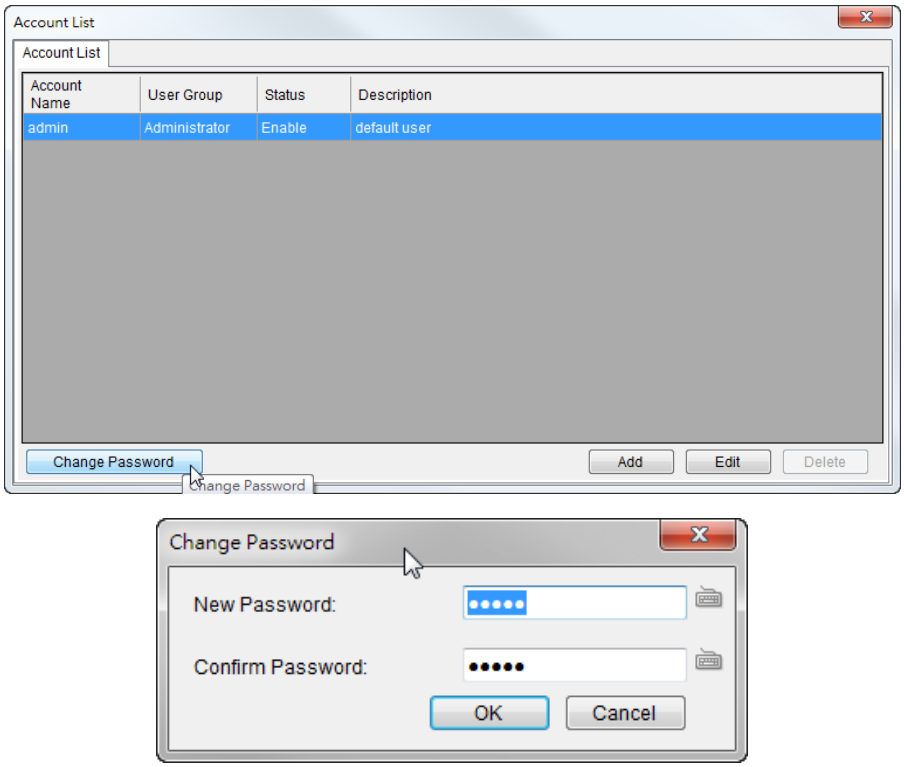
5. If desired check the **Disable User** box to disable this account.

6. Click **Ok** to save the changes to the account. If the account description, user group or status changes, it will be reflected in the *Account List*.

Changing an Account Password

In addition to editing the password from using the *Account List* editing function, the password for the current account can also be changed by clicking the **Change Password** at the lower left corner of *Account List Window*.

This will display a dialog that allows you to enter and confirm a new password.



Deleting an Account

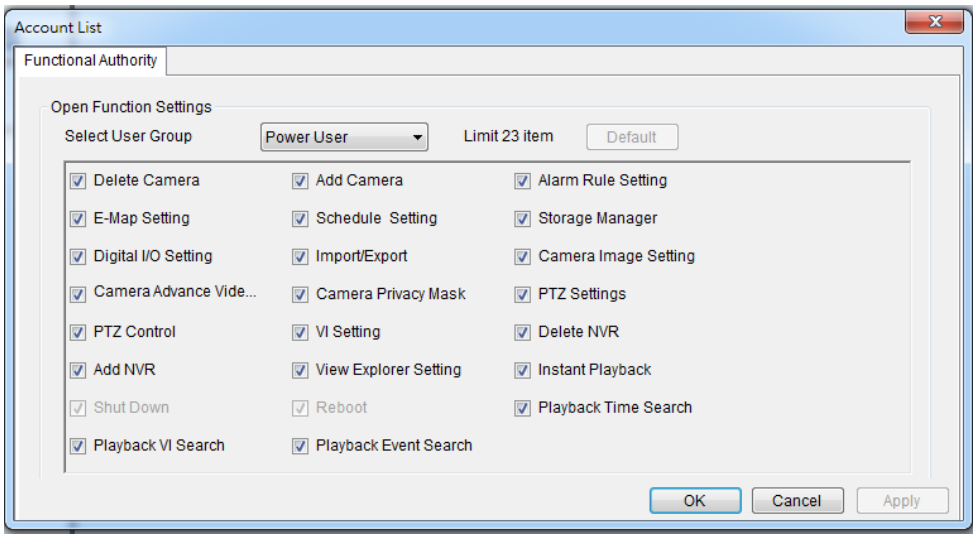
To delete an account to the domain:

1. Access the *Account List* node in the *SCC Console*.
2. Select the account that you wish to delete by clicking on the account.
3. Click the **Delete** button at the bottom of the *Account List* screen.
4. When prompted to confirm deletion click **Yes** to delete the account. The deletion will be reflected in the *Account List*.

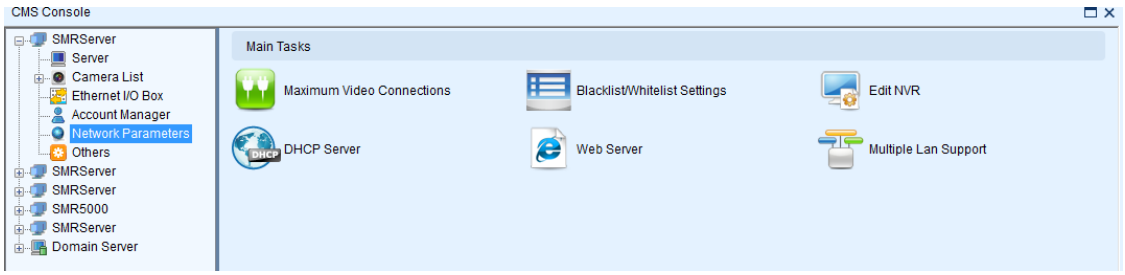
Note: The *Admin* account cannot be deleted.

10.5.2. Functional Authority

Functionalities can be authorized according to different user levels.



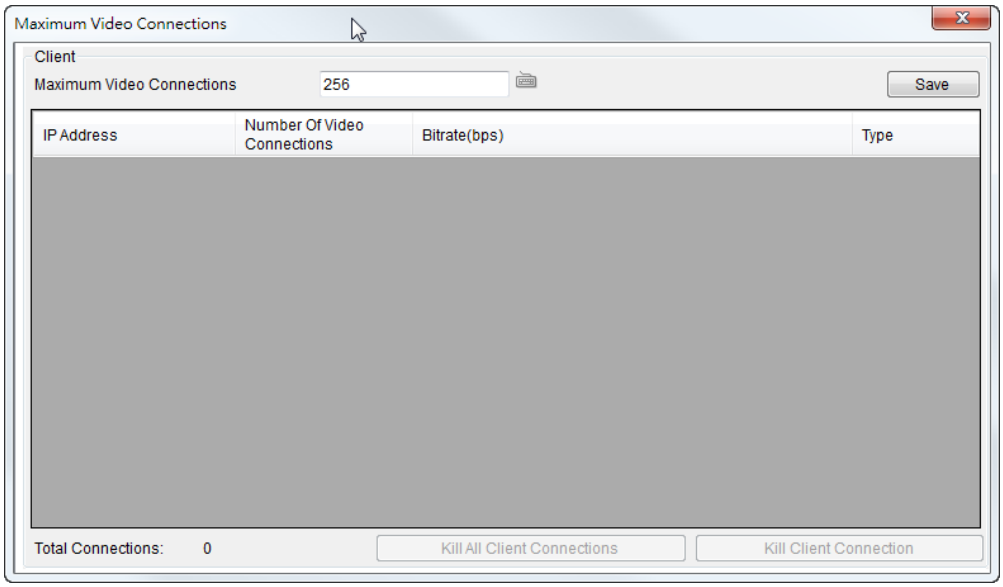
10.6. Settings Under Network Parameters



10.6.1. Main Tasks

Here you can access shortcuts for network parameter settings.

Maximum Video Connections



When clients are connected the following information will be displayed for each client:

- **IP Address**
- **Number of Video Connections** - The number of streams that the client is using.
- **Bitrate** - The total bitrate of that the client is consuming.
- **Type**

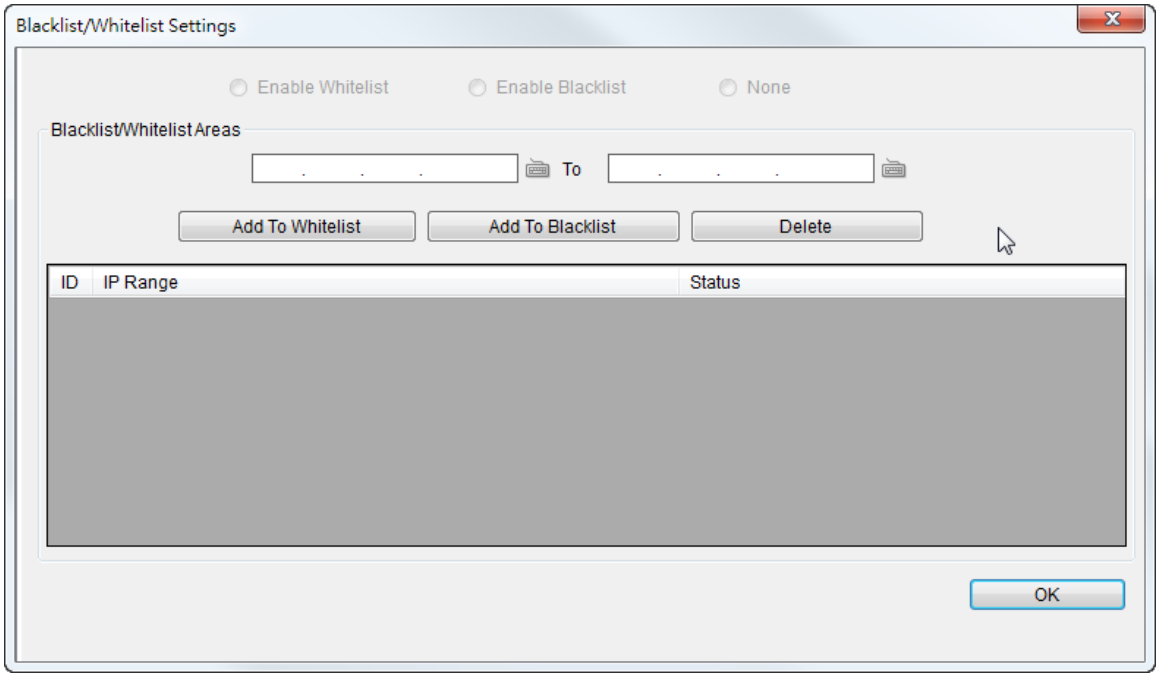
There are also some options that can be changed in this dialog:

- **Maximum Connections** - Change this number to limit the total number of video connections. Default is 256. Click **Save** to save the changes.
- **Kill All Client** - This button disconnects all clients connected on the Server.

- **Kill Client** – Selecting a client from the client list and clicking this button will disconnect the client from the Server.

Blacklist/Whitelist Settings

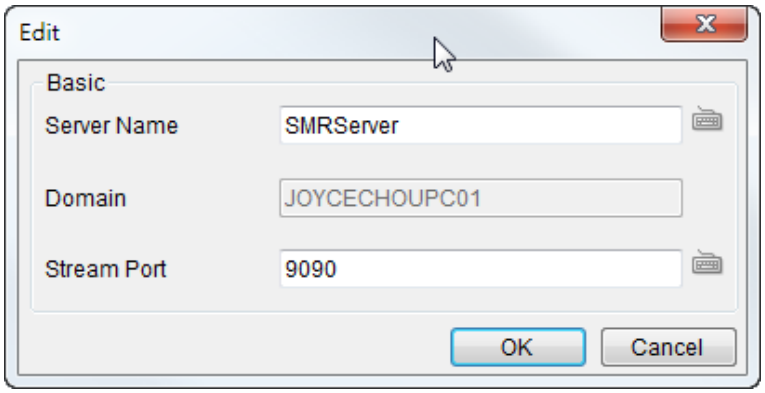
To setup a blacklist or whitelist:



1. Enter an IP range in the two IP fields. The first IP address should be lower than the second IP address.
2. Click either **Add to Whitelist** or **Add to Blacklist** to add the IP range to the whitelist or blacklist respectively.
3. Repeat the first two steps to set up the blacklist and whitelist. You can select ranges that have already been configured from the list and click **Delete** to delete them.
4. When completed, click either **Enable Whitelist** to allow only the IP ranges on the whitelist to access the Server, or **Enable Blacklist** to block all the IP ranges on the blacklist from accessing the Server.
5. Click **OK** to save your changes.

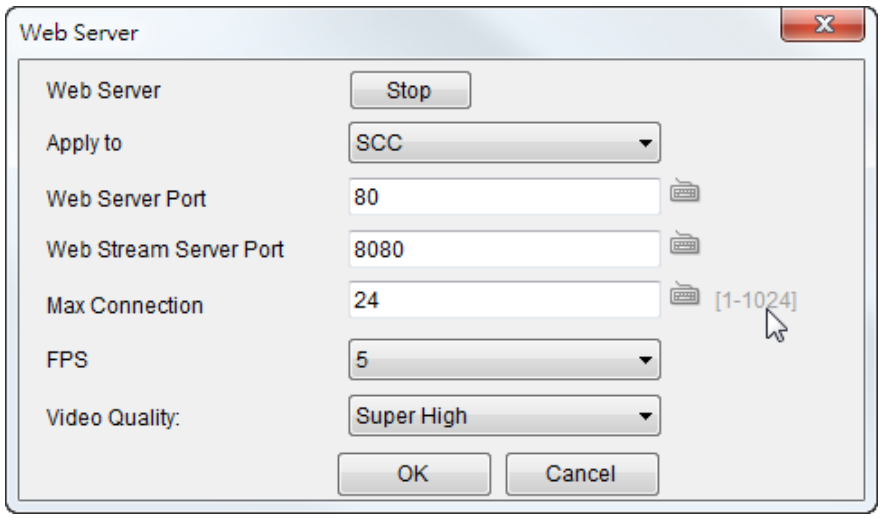
Edit NVR

Users can change both the setting of the stream port and the IP address by editing the Server.



Web Server

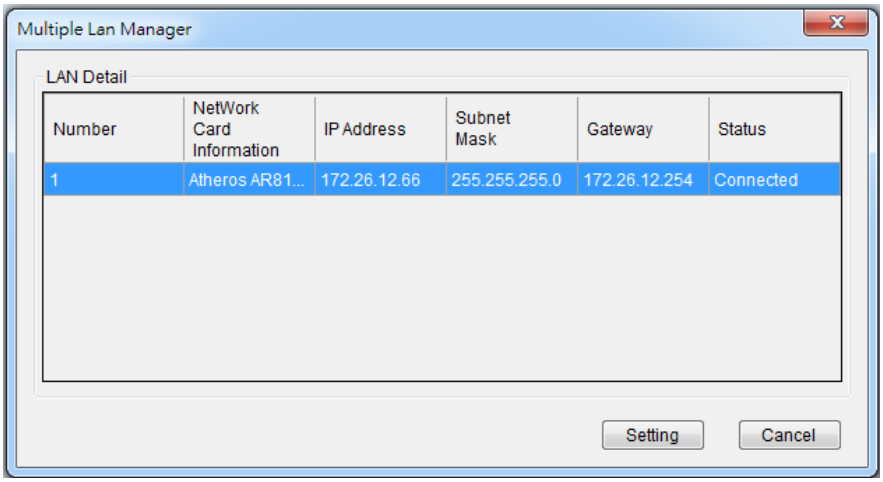
For users who want to use the Web Client, please fill in the following information for the Web Server settings.



Note: User may just keep the default settings in the Web Server.

Multiple LAN Support

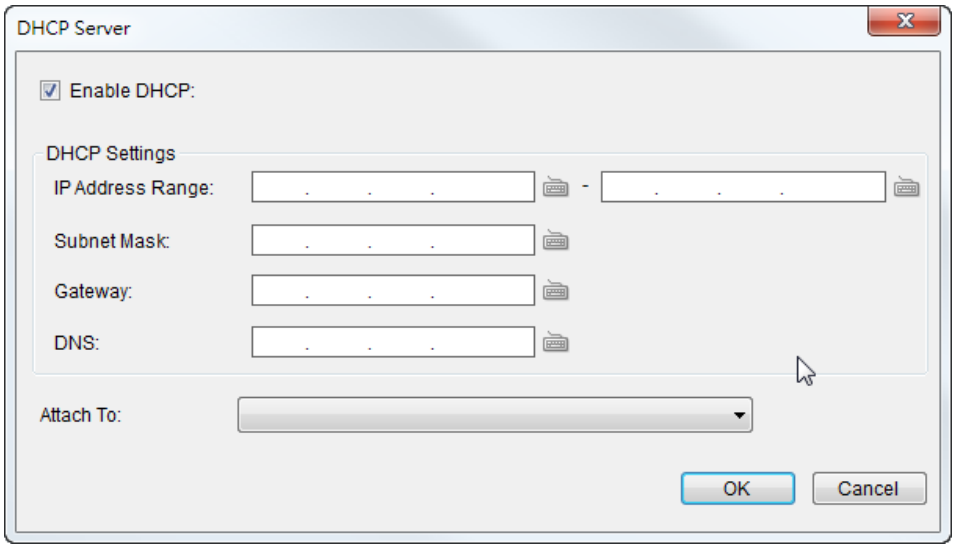
Multiple network cards can be supported. Their information is listed as below:



Click the **"Setting"** to set the Network Card to DHCP Auto-Configuration or Fixed IP Address.

DHCP Server

The SCC has built in DHCP server functionality. Although this function is disabled by factory default, it should be turned on in the event that there is no DHCP service available. When enabled, the SCC will assume DHCP Server duties and assign addresses within the range specified.



Note: You may skip this step if you have separate DHCP service. Most routing devices will have DHCP capabilities.

1. Right-click the SCC Server and select ***Configurations*** > ***DHCP Server*** option to bring up the *DHCP Server* dialog box.

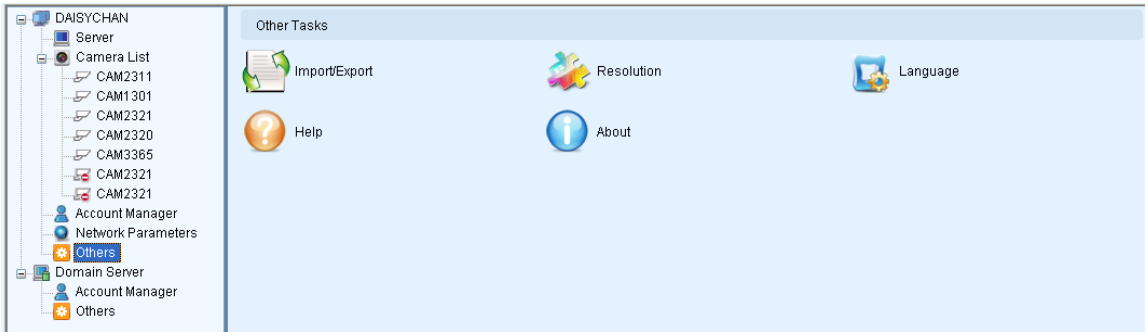
2. Fill in the following information:

   - **IP Address Range** - The range of addresses to be assigned. The first IP address should be lower than the second IP address.
   - **Subnet Mask**
   - **Gateway** – The gateway IP
   - **DNS** – The DNS IP

Note: DHCP service can also be configured by clicking ***SMR Server*** > ***Configuration*** > ***DHCP Server***.

Note: The DHCP service should be attached to a network card.

10.7. Settings Under Others

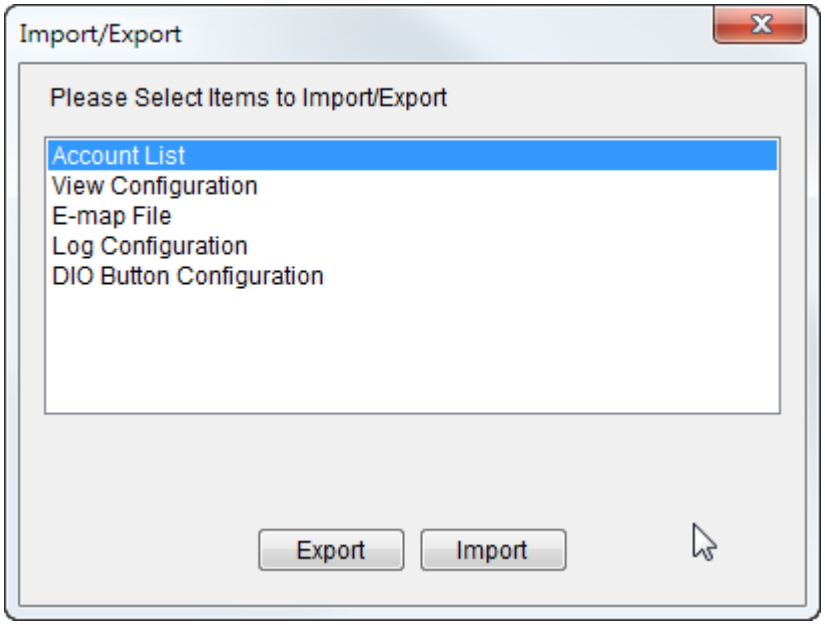


10.7.1. Other Tasks

Here you can access shortcuts for miscellaneous settings.

Import/Export

The following types of configuration/setup files can be imported/exported to the Server:



- **Account List**
- **View Configuration**
- **E-map File**
- **Log Configuration**
- **DIDO Button Configuration**

Importing Parameters

To import parameters into the Server:

1. Select the item that you wish to import by clicking on the item type.
2. Click the **Import** button. A windows explorer dialog will appear.
3. Select the file to import from the file explorer, and click **Open** to import the file.
4. Click **OK** to confirm import. The Server will require a restart before imported configurations and files are applied.

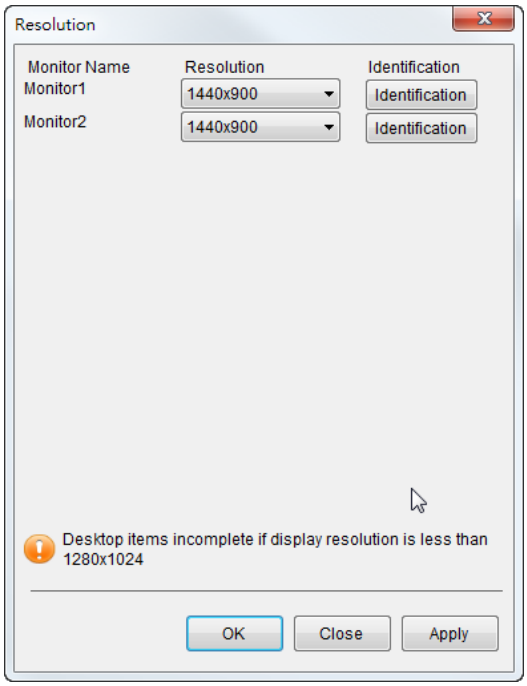
Exporting Parameters

To export parameters into the Server:

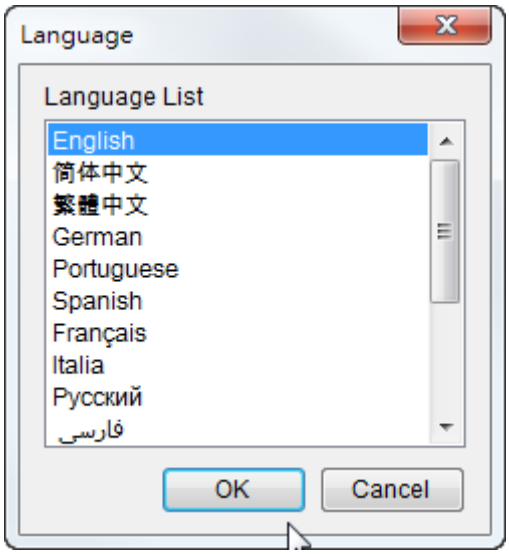
1. Select the item that you wish to export by clicking on the item type.
2. Click the **Export** button. A windows explorer dialog will appear.
3. Input a filename and select the export path in the file explorer, and click **Save** to export the file.

Resolution

Shows the monitor resolution, and allows you to change its setting.



Language



Allows you to change the interface language.

Help

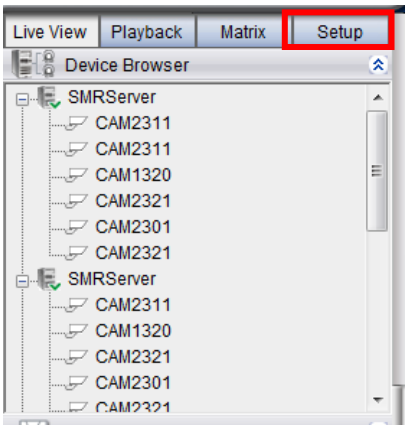
Allows you to access the SCC User Manual.

About

Allows you to view server and client information.

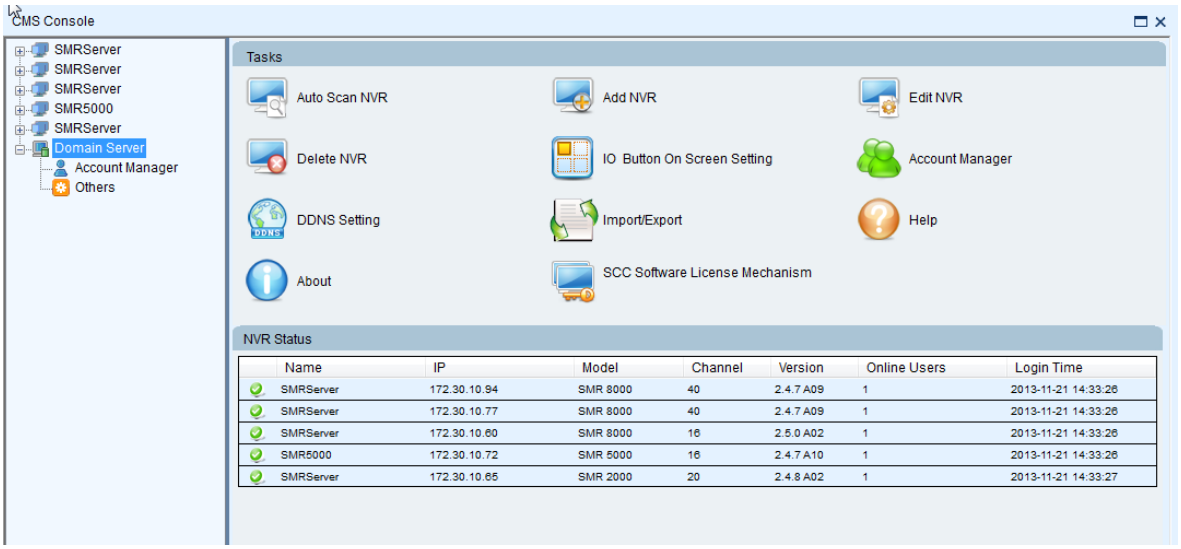
10.8. Settings Under Domain Server

Select Setup Button on the menu bar.



The SCC Console shows up listing shortcuts to commonly used functionalities, system status, and recent events.

Select Domain Server from the side bar. The home page appears, listing shortcuts to commonly used functionalities and system status.

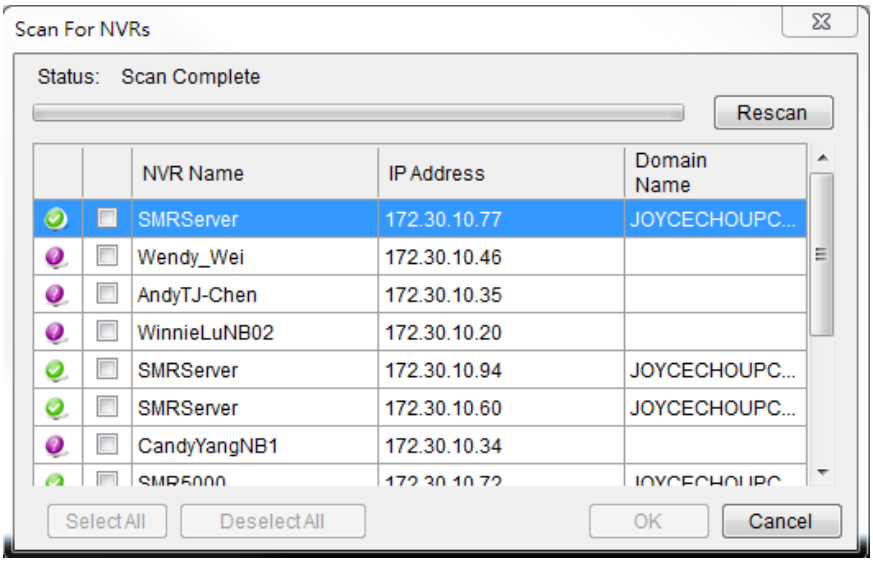


Tasks

Lists shortcuts to frequently accessed server functionalities.

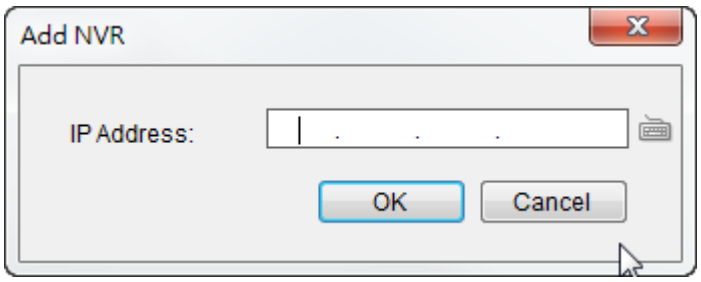
Auto Scan NVR

Scans for the existing NVR Servers. NVR can only be logged in to 1 SCC /VMS. Before adding NVR in, go to the Server Console Page and select clear SCC / VMS Data to clear old data in the original SCC / VMS management software.



Add NVR

NVR Server can be added by entering the Server IP.



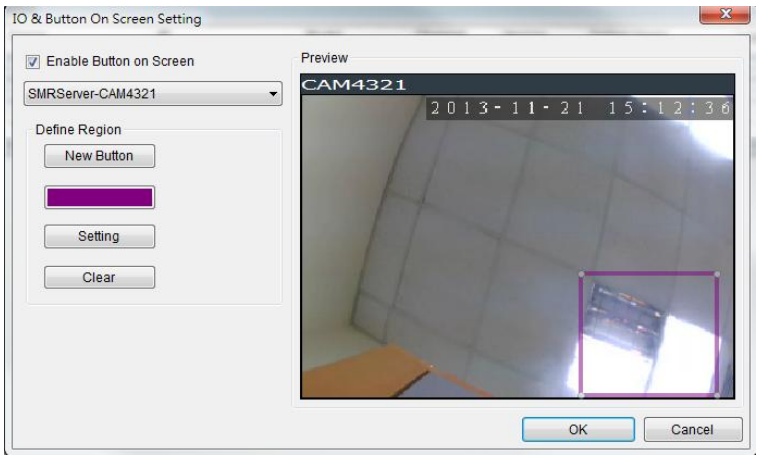
Edit NVR

Users can change both the setting of the stream port and the IP address by editing the Server.

Delete NVR

The added NVR Server can be deleted.

IO Button On Screen Setting



SCC can also control the Input / Output devices, when you have the IO devices connected to the camera.

Set the IO Button On Screen Setting allows you to control the IO on screen. For example, you can set the detection area on the lamp, when you need the lights on, just click on the set area on screen and the lamp will be triggered to on/off.

1. Check the **Enable Button on Screen**.

2. Select the camera with IO devices connected.

3. Click on the "**New Button**" to define the detection area.

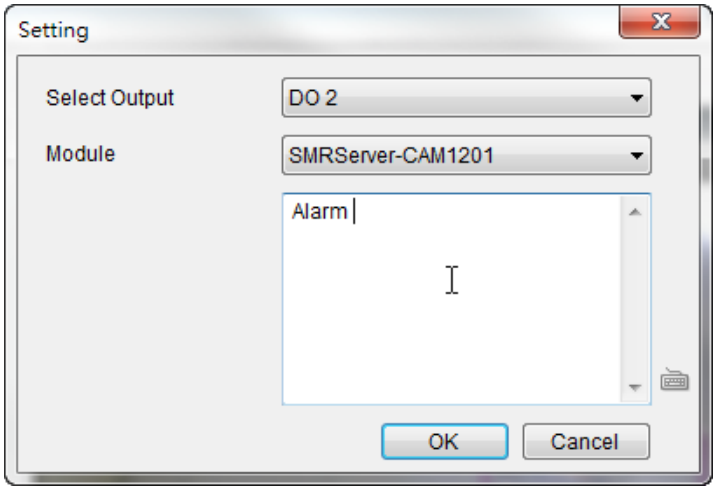
4. Color of the area can be further defined. When you have more than one IO devices need to be triggered, this will be very useful.

5. Click "**Setting**", the following window will be prompted out.

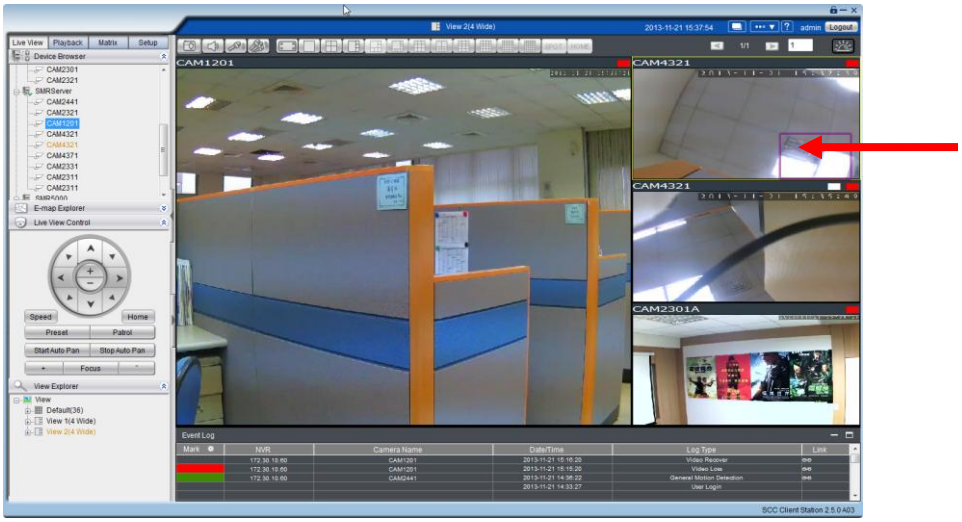
This setting allows you to trigger the IO devices on the other cameras as long as they are all connected with one another.

For example, the set camera CAM4321 doesn't have alarm device as DO, but the other camera CAM1201 has it. We can set the IO Button on the CAM4321 to trigger the DO on the CAM1201.

Select the module and the connected output devices from the "**Select Output**" dropdown list and then put some descriptions in the blank for this setting.



You can see the IO Button on the screen after the setting.



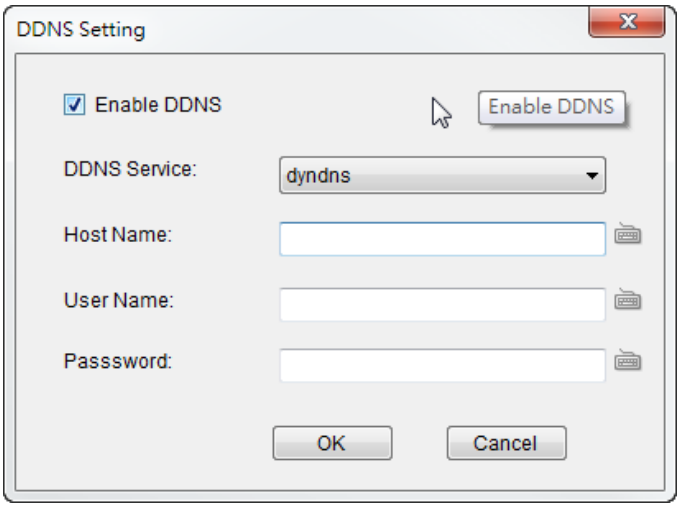
Now you can click on the IO box to trigger.

Double click the image to maximize the screen and double click again to minimize.

Account Manager

Account management for the domain can be performed under the *Account Manager* > *Account List* node. Under this dialog, you may add, delete, and edit domain users. See *Account Manager* for more details.

DDNS Setting



DDNS (Dynamic Domain Name Server) is a protocol that enables the camera to maintain a static connection address, even when its IP changes. Access using this feature is disabled by default.

Connecting using DDNS requires registration on third-party websites for DDNS services. Select desired DDNS service website, check the **Enable DDNS** option, and fill in valid user name and password. You can then access the camera through the registered domain name.

Import/Export

Configuration/setup files can be imported/exported to the server. See *Server Setup > Other Tasks > Import/Export or Other Parameters > Other Tasks > Import/Export* for more details

Help

Allows you to access the SCC User Manual.

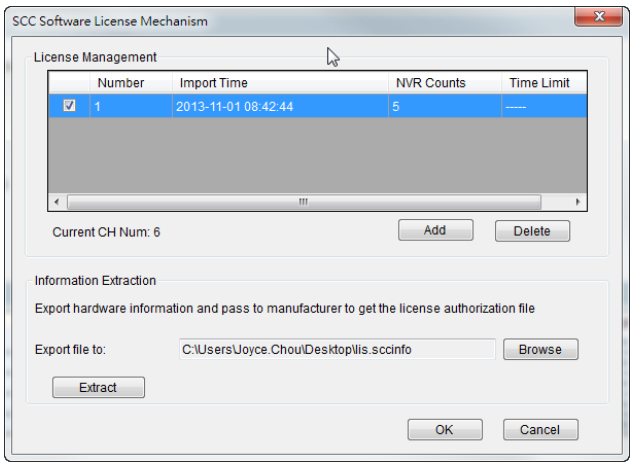
About

Allows you to view server and client information. See *Server Basic Functions > Viewing Server and Client Information* for more details.

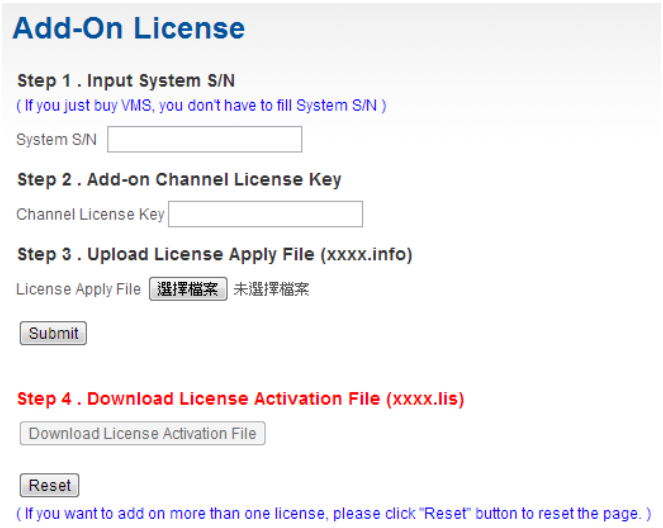
SCC Software License Mechanism

Extra supported channels can be added by purchasing licenses. After the purchase, you need to register to add the extra channel.

1. Click **Browse.** You can rename the file and select a path for the original channel information.



2. Click **Extract**. The *.sccinfo file will be stored to the selected path or to the default path usually your desktop.
3. Go to http://www.surveon.com/license/license.aspx to see the Add-On License page and follow the steps for the online registration.


Add-On License
Step 1 . Input System S/N
(If you just buy VMS, you don't have to fill System S/N)
System S/N
Step 2 . Add-on Channel License Key
Channel License Key
Step 3 . Upload License Apply File (xxxx.info)
License Apply File
選擇檔案
未選擇檔案
Submit
Step 4 . Download License Activation File (xxxx.lis)
Download License Activation File
Reset
(If you want to add on more than one license, please click "Reset" button to reset the page.)

- **Step 1: Input System S/N**
  Find the S/N on your SMR / NVR device and input the S/N.
  For SCC / VMS, there will be no series number, go to the next step.
- **Step 2. Add-on Channel License Key**
  Find the license key on the Software Add-on License Certificate and input the license key.

- **Step 3. Upload License Apply File (xxx.info)**
  Click "**Browse**" to select the extracted file and then click "**Submit**".
- **Step 4. Download License Activation File (xxxx.lis)**
  Click "Download License Activation File" to download the file.
  This file will be used later on.

The file name is generated by the system. Its naming rule is "**S/N+License Key+Channel Number.lis**". For SCC / VMS, there will be no series number, its naming rule will be "**License Key+Channel Number.lis**".

Click "**Reset**" if you have more than one license to add on. Follow the previous steps to complete the registrations.

4. After receiving the license file, go back to the SCC Console under Domain Server and click **ADD** to upload your "xxx.lis" file from the online registration to SCC.
5. Check the License Management to make sure if the channels are added successfully. Once your purchased channels are added on, click "OK" to confirm and leave this page.